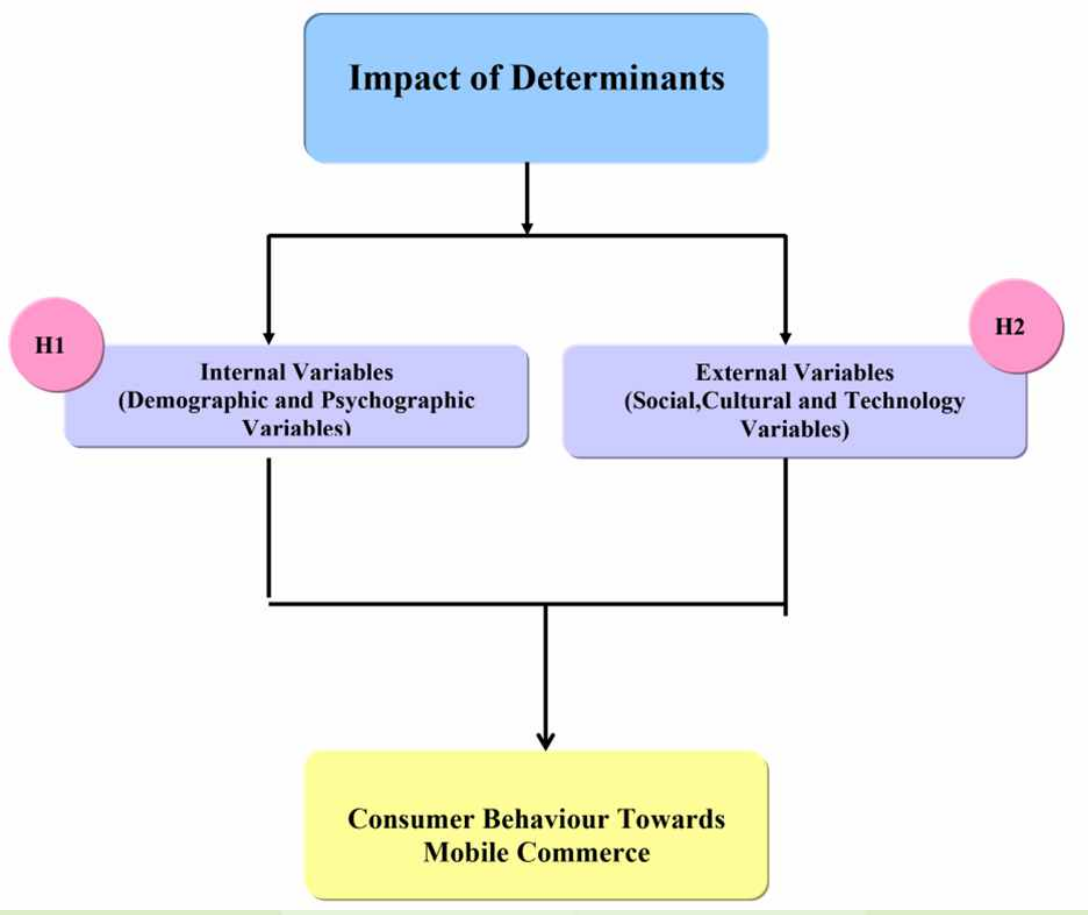
ISSN: 1913-3715 Volume 8, Number 13, December 2015

Scientific Research Publishing

International Journal of Communications, Network and System Sciences



ISSN: 1913-3715
9 771913 371006 13

www.scirp.org/journal/ijcns

JOURNAL EDITORIAL BOARD

ISSN 1913-3715 (Print) ISSN 1913-3723 (Online)
http://www.scirp.org/journal/ijcns

Int. J. Communications, Network and System Sciences, 2015, 8, 523-596
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns

Scientific Research Publishing

Table of Contents

Volume 8 Number 13 December 2015

The figure on the front cover is from the article published in Int. J. Communications, Network and System Sciences, 2015, Vol. 8, No. 13, pp. 578-596 by Arif Sari and Pelin Bayram.

International Journal of Communications, Network and System Sciences (IJCNS)

Journal Information

SUBSCRIPTIONS

The *International Journal of Communications*, *Network and System Sciences* (Online at Scientific Research Publishing, www.SciRP.org) is published monthly by Scientific Research Publishing, Inc., USA.

Subscription rates:
Print: $89 per issue.
To subscribe, please contact Journals Subscriptions Department, E-mail: sub@scirp.org

SERVICES

Advertisements
Advertisement Sales Department, E-mail: service@scirp.org

Reprints (minimum quantity 100 copies)
Reprints Co-ordinator, Scientific Research Publishing, Inc., USA.
E-mail: sub@scirp.org

COPYRIGHT

SPONSOR:

International School of Software, Wuhan University (iss.whu.edu.cn).

PRODUCTION INFORMATION

For manuscripts that have been accepted for publication, please contact:
E-mail: ijcns@scirp.org

Int. J. Communications, Network and System Sciences, 2015, 8, 523-532
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813047

Scientific Research Publishing

Performance Analysis of Grid Based AODV Routing Algorithm for AD Hoc Wireless Networks

Abderezak Touzene, Ishaq Al-Yahyai

Computer Science Department, Sultan Qaboos University, Muscat, Oman
Email: touzene@squ.edu.om, ishaq@gmail.com

Received 11 November 2015; accepted 27 December 2015; published 30 December 2015

Abstract

In many traditional On Demand routing algorithms in Ad hoc wireless networks, a simple flooding mechanism is used to broadcast route request (RREQ) packets when there is a need to establish a route from a source node to a destination node. The broadcast of RREQ may lead to high channel contention, high packet collisions, and thus high delay to establish the routes, especially with high density networks. Ad hoc on Demand Distance Vector Routing Protocol (AODV) is one among the most effective Reactive Routing Protocols in MANETs which use simple flooding mechanism to broadcast the RREQ. It is also used in Wireless Sensor Networks (WSN) and in Vehicular Ad hoc Networks (VANET). This paper proposes a new modified AODV routing protocol EGBB-AODV where the RREQ mechanism is using a grid based broadcast (EGBB) which reduces considerably the number of rebroadcast of RREQ packets, and hence improves the performance of the routing protocol. We developed a simulation model based on NS2 simulator to measure the performance of EGBB-AODV and compare the results to the original AODV and a position-aware improved counter-based algorithm (PCB-AODV). The simulation experiments that EGBB-AODV outperforms AODV and PCB-AODV in terms of end-to-end delay, delivery ratio and power consumption, under different traffic load, and network density conditions.

Keywords

Mobile Ad-Hoc Networks, AODV Routing Algorithm, Position-Based Routing, Grid-Based Routing, NS2

1. Introduction

A Mobile Ad Hoc Network (MANET) is a collection of wireless nodes communicating with each other in the

How to cite this paper: Touzene, A. and Al-Yahyai, I. (2015) Performance Analysis of Grid Based AODV Routing Algorithm for AD Hoc Wireless Networks. *Int. J. Communications, Network and System Sciences*, **8**, 523-532.
http://dx.doi.org/10.4236/ijcns.2015.813047

absence of any fixed infrastructure. Efforts have been taken for achieving efficient routing protocols in mobile ad hoc networks. Routing in a mobile ad hoc network is a challenging task since the network's topology is dynamic due to nodes mobility. In many on-demand routing protocols, a node sends a route-request control packets to establish and maintain a route to a given destination. Since the overall available network bandwidth and node power are limited, the routing-related control packets should be minimized. Therefore, route establishment and maintenance mechanisms should minimize the number of control packets to reduce the end-to-end delay and also minimize the battery consumption power and thus improve the mobile nodes lifetime.

In [1], the routing protocols for Ad hoc networks are classified depending upon whether route is updated continuously or on-demand. The proactive class: try to maintain consistent and up-to-date routing information from each node to every other node in the network; the reactive class: routes are requested on-demand only when they are needed; and the hybrid class: combines the advantage of both proactive and on-demand protocols. To maintain up-to-date routing table information, proactive protocols generate periodic control packets which lead to a high communication overhead and thus could not be suitable for use in ad hoc network scenarios where the network density is large and where the topology may change frequently. For such scenarios on-demand routing protocols are preferable.

Conventional on-demand routing protocols such as Dynamic Source Routing (DSR) [2], Ad Hoc on Demand Distance Vector (AODV) [3], Zone Routing Protocol (ZRP) [4], and Location Aided Routing (LAR) [5], try to establish a route between a source and a destination when it is needed by broadcasting using a simple flooding operation to disseminate a route request RREQ. In a simple flooding operation, an RREQ packet is transmitted to the nodes within its transmission range. All the nodes receiving the RREQ will rebroadcast the message if they see it for the first time. This rebroadcast strategy leads to high network contention and collision because many nodes will be involved in the rebroadcast operation. This problem is known as the broadcast storm.

Efforts have been taken for achieving efficient broadcasting in mobile ad hoc networks. Network broadcasting is the process in which one node sends a packet to all other nodes in the network. Broadcasting in MANETs constitutes one of the fundamental network operations which serve various network services including: routing, information dissemination and resources discovery. As an example, several unicast routing protocols such as DSR, AODV, ZRP, and LAR, as well multicast protocols employ broadcasting to detect and maintain routes in a dynamic environment. Because many network services have stringent end-to-end delay requirements, the design of low-latency and low overhead broadcasting schemes is essential to many practical applications.

Recently, in [6] we proposed an efficient Extended Grid Based Broadcast algorithm EGBB which solves the broadcast storm problem in MANET. EGBB sees the terrain as a logical 2D grid with $k \times k$ grid cells. The main idea of EGBB resides in its rebroadcast strategy where only a gateway node (one per grid cell) will rebroadcast the packet. A gateway node is set dynamically and it can be any node. A normal node S1 in a given cell can be seen (or upgraded) as a gateway node for a node R located in another cell if it has seen (received) any kind of traffic from the node S1. Later if R receives any traffic from a node S2 located in the same cell as S1 it will be upgraded to gateway node in that cell instead of S1. It has been shown in [6] that EGBB has outperformed up-to-date broadcasting algorithm in MANET.

Ad hoc on Demand Distance Vector Routing Protocol (AODV) is one among the most effective Reactive Routing Protocols in MANETs. It is also used as routing protocol in Wireless Sensor Networks (WSN) [7] and in Vehicular Ad hoc Networks (VANET) [8]. Vehicular Ad Hoc Network VANET is becoming more and more important, which can provide intelligent transportation application, comfort application and other services for people in vehicles.

In this paper, we propose a new variation of AODV routing algorithm named EGBB-AODV which conserves most of the ideas of AODV but we change the RREQ mechanism originally using simple flooding and replace it with EGBB broadcasting.

The remainder of the paper is organized as follows: Section 2 presents some related work; Section 3 presents an overview of the proposed EGBB-AODV algorithm; Section 4 presents simulation model and some performance results; and Section 5 concludes the paper.

2. Related Work

Many route discovery protocols, found in the literature [9]-[15] proposed efficient protocols to optimize the route discovery MANETs. The proposed schemes alleviate the impact of the broadcast storm problem by re-

fraining some nodes from re-broadcasting and favoring others depending on probability, their location, and their knowledge of how many times the message has been broadcasted. In [16], the authors developed a cross-layer approach focusing on the Signal-Strength based Medium Access Control protocol to orchestrate the channel access based in MANETs. Another cross-layer approach is presented in [17] where a multipath routing protocol for MANET based on On-Demand Distance Vector (AODV) routing protocol to reduce the end-to-end delays.

A broad category of routing and broadcasting algorithms is the class of position-based algorithms [18]-[22]. These algorithms make use of the nodes' geographical positions to make routing decisions. Nodes are able to obtain their own geographical positions via Global Positioning System (GPS). This approach has become practical by the rapid development of low cost hardware and software solutions for determining absolute or relative node positions in MANETs [23].

In this paper we proposed an improvement for AODV routing protocol called EGBB-AODV routing algorithm which replaces the original RREQ simple flooding mechanism by a most sophisticated broadcast EGBB for forwarding the route request packets RREQ. In the EGBB-AODV algorithm, it is assumed that each node knows only its position using a Global Positioning System (GPS). Nowadays, mobile computing devices and smart phones are all equipped with such GPS system. The geographical region of the MANET is viewed as a logical 2-dimensional (2D) grid of cells as shown in **Figure 1**. With the help of the EGBB broadcast procedure, the initiator of the RREQ message within a given cell broadcasts its message to nodes located in its neighborhood cells based on the node's transmission range. This first step consists of a local broadcast or one-hop broadcast. In the second step of the EGBB algorithm, only one node (gateway node) per grid cell rebroadcasts the RREQ message. In the flooding algorithm, all the nodes which receive the message will rebroadcast the RREQ it (broadcast storm problem). In EGBB-AODV, the problem of broadcasting RREQ to mobile MANET nodes is transformed into a problem of broadcasting to geographically fixed grid cells using only the gateway nodes as RREQ rebroadcast nodes. Typically, each node will have a dynamic list of eight gateway nodes (one gateway node for each cardinal direction). A RREQ packet is rebroadcasted from a gateway node in a grid cell to nodes in neighboring grid cells within the node's transmission range repeatedly until it reaches all nodes in the 2D grid.

3. EGBB-AODV Protocol

Node will have in what follows we give a brief description of the original routing algorithm AODV, and the two broadcast algorithms candidates for replacing the simple flooding of RREQ in the improved AODV: Extended Grid-Based Broadcast EGBB [6] and the Position-aware Counter-Based algorithm (PCB) [24].

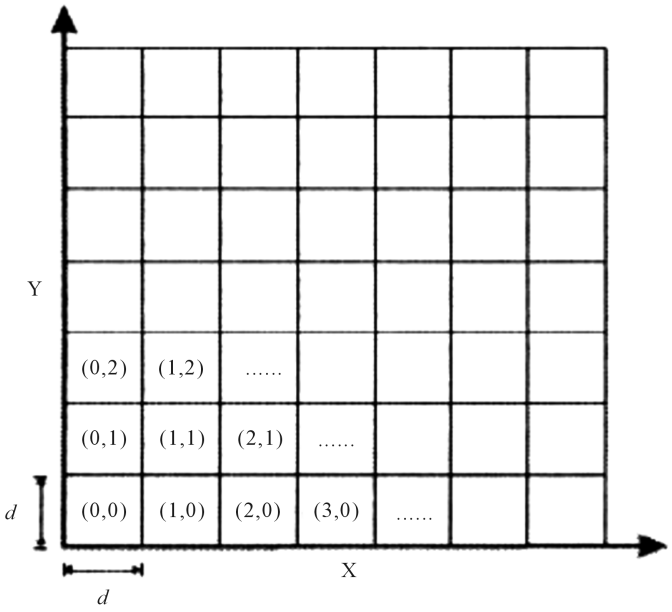


Figure 1. Logical 2D view of the area.

3.1. Overview of AODV

AODV is an on-demand routing algorithm that determines a route only when a node wants to send a packet to a destination. The route discovery process is started whenever a source node wants to communicate with a destination node for which it has no routing information (routing table). The source node initiates a path discovery by broadcasting a route request (RREQ) packet to its immediate neighbors. Each neighbor either satisfies the RREQ by sending a route reply (RREP) back to the source if it knows the path to destination or rebroadcasts the RREQ to its own neighbors if the RREQ is seen for the first time. Each intermediate node that forwards the RREQ packet creates a reverse route pointing towards the source node. When the intended destination node or an intermediate node with a valid route to the destination receives the RREQ packet, it replies by sending a route reply (RREP) packet. The RREP packet is unicast towards the source node along the reverse path set-up by the forwarded RREQ packet. Each intermediate node that participates in forwarding the RREP packet creates a forward route (entry in the routing table) pointing towards the destination. Once the next hop becomes unreachable, the node upstream from the breaking point propagates a route error packet RERR to all active upstream neighbors. Those nodes subsequently relay that message to their active neighbors and so on. This process continues until all active source nodes are notified. Upon receiving notification of a broken link, source node can restart the discovery process if it still requires a route to the destination. RREP packets are also sent when an entry in a routing table expires (relatively old route).

3.2. Extended Grid Based Broadcast EGBB

EGBB is an efficient broadcast algorithm for MANET [6] which uses a logical 2D grid representation of the terrain as a $k \times k$ grid cell of side d (see **Figure 1**).

Each grid cell has eight adjacent of neighboring grid cells (share a side or a corner), except the cells at the boundaries. For a given grid cell, the eight neighboring grid cell are identified using the cardinal direction. NorthWest grid cell GW[0], North grid cell GW[1], NorthEast grid cell GW[2], East grid cell GW[3], SouthEast grid cell GW[4], South grid cell GW[5], SouthWest grid cell GW[6], and East grid cell GW[9]. Each node in EGBB maintain continuously its list of eight gateway nodes corresponding to potential rebroadcast nodes in each neighboring grid cell (GW[0..7]). The list of gateway nodes GW is updated when a node hear any kind of traffic from a neighboring node in a neighboring grid cell. It will compute the sender node direction i using the sender position extracted from the received packet and updates its list of gateways GW[i] = idr where idr is the ID of the sender extracted from the received packet. When a node broadcast the packet it will add to the packet the list of gateways GW. When a node receive a broadcast packet it checks if its ID is among the GW list in the received packet in this case it will rebroadcast the message. Otherwise it will just consume the packet. The broadcast packet in EGBB is relayed only by the gateway nodes. This rebroadcast strategy is reduces the number of rebroadcast in each hop eight rebroadcast nodes per hop independently from the network density.

3.3. Position-Aware Counter-Based Algorithm (PCB)

PCB algorithm integrates the merits of counter-based and position-based schemes. When a node rebroadcasts a packet, it adds its own position to the header of the packet. When receiving a duplicated packet, it gets the position of the sender and recalculates its Expected Additional Coverage (EAC). A node rebroadcasts a packet only when the EAC) is larger than a certain threshold. Within PCB, threshold values of expected additional coverage and counters vary adaptively according to network density. Threshold value for counters of nodes in sparse networks is set differently from that in dense networks

As described in [24], the first (EAC) threshold V1 is set to 40% of the transmission range and the second EAC threshold V2 is set to 60% of the transmission range. The counter threshold Cth is set to 3 as in PCB algorithm. PCB implements two different RAD periods: a long RAD period LRAD for node located with range greater than V1 and less than V2. A shorter RAD period SRAD for nodes located in the range greater than V2. The nodes located in the later range will rebroadcast before the node located in the former range because of their shorter RAD period. This will be in favor of nodes with higher EAC and thus ensure better performance.

PCB Algorithm [24]

```
-On hearing a broadcast packet m at any node X
- Get the position information of previous node from m
- For new packet m received at X, calculate EAC [24]
if EAC > V1
{
 if m is a new packet
  {
   initiate C = 1
   if EAC > V2 Set and wait for RAD=SRAD (short RAD) to expire
   else Set and wait for RAD=LRAD (Long RAD) to expire
  }
} else drop m
- For every duplicate packet m received within RAD, calculate EAC
if EAC > V1 increment C, C=C+1;
- RAD expires
if C < Cth rebroadcast m
  else drop m
```

3.4. EGBB-AODV

We propose a new variation of AODV routing algorithm named EGBB-AODV which conserves most of the ideas of AODV but we changed the RREQ mechanism originally using simple flooding and replace it with EGBB broadcast algorithm. EGBB-AODV sees the terrain as a logical 2D $k \times k$ grid cell of side d (see **Figure 1**).

Whenever a RREQ packet is generated by EGBB-AODV it will be broadcast using EGBB to reduce the number of rebroadcast and improve the performance of the new modified protocol. Some beneficial features have been added in EGBB-AODV to deal with some control packets such as route reply RREP and route error RERR. When a RREP is generated at the destination node, the information about RREP packet are used to maintain the list of gateways in the receiving or intermediate node located in neighboring grid cells. We do similar gateway updating when a node receives RERR. EGBB-AODV relay on any kind of traffic generated the nodes, RREQ, RREP, RERR, data, to maintain an up-to-date list of gateway GW[0..7]. This gateway updates does not incur any extra-cost compared to the original AODV algorithm.

For comparisons purpose, we implemented a new version PCB-AODV which uses PCB as the broadcast algorithm to disseminate the RREQ.

4. Performance Analysis

In what follows, we study the performance for the three routing protocols the original AODV, EGBB-AODV and PCB-EODV using Ns2 simulator. The performance metrics we are interested to analyze are as follows:

- The average end-to-end delay, the average time spent to complete one routing operation.
- The average reachability ratio, the average percentage of nodes that received the messages.
- The power consumed by a node, total number of packet (data and control packet) transmitted by a node per second.

For all simulation scenarios, all nodes move according to the random waypoint mobility model where the velocity of nodes is chosen uniformly from 0 to 12 m/s and the pause time is set to zero. All nodes start to move at the beginning of the simulation and do not stop until the end of simulation. The source nodes of CRB traffic are chosen randomly over the network allowing simultaneous CBR traffic operations from different sources. Identical mobility scenarios and traffic patterns are used across simulation scenarios in order to achieve a fair comparison. The simulation time is set to 1000 s and the first 100 s are discarded in order to be sure that the network has reached the steady state. All simulation results are obtained with 95% confidence interval and relative error less than 5%. The simulation model does not take into account the effect of environment such as buildings, mountains, etc. [25]. **Table 1** gives a summary of the simulation system parameters. The radio propagation model used in this study is the NS2 default, which uses characteristic similar to a commercial radio interface,

Table 1. Simulation parameters.

Area	1000 m × 1000 m
Protocols	AODV, EGBB-AODV, PCB-AODV
Mobility model	Random waypoint
Numb. of nodes	100, 200, 300
Nodes speed	3, 12, 24 m/s
Avg. pause time	0
CBR/sec.	1, 6, 12, 24 Pkt/sec
Trans. range	300 meters
Link bandwidth	2 Mbps
Simulation trials	30 times
Simulation time	1000 Seconds

Lucent's WaveLAN card with a 2 Mbps bit rate [26]. The distributed coordination function (DCF) of the IEEE 802.11 protocol [27], [28] is utilized as MAC layer protocol while random waypoint model [29] is used as the mobility model.

4.1. Effect of the Traffic Load

In this set of simulation experiments we fix the number of nodes to 100 and the node mobility to an average of 12 m/s (high mobility). We vary the number of CBR traffic per second and study the average end-to-end delay time, the delivery ratio, and the average power consumption per node per second.

Figure 2 shows a considerable improvement on the end-to-end delay of EGBB-AODV compared to AODV and PCB-AODV, especially when the traffic increases. EGBB-AODV finds routes faster than AODV and PCB-AODV because it involves less rebroadcast of RREQ and thus less collisions. Collision may prevent RREQ to reach the destination. AODV implements a retrial procedure to send again the RREQ if any RREP is not received within a given time out. **Figure 3** shows that EGBB-AODV has better delivery ratio compared to the traditional AODV and PCB-AODV. It shows also that when the traffic is high (24 pkts/s) the delivery ratio of AODV drops to 60%, and PCB-AODV drops to 72% when the delivery ratio of EGBB-AODV is within 80%. **Figure 4** reveals that the good performance of EGBB-AODV over AODV and PCB-AODV in terms of saving the battery energy. It also shows that with the increase of the traffic the battery consumption is increased for the three algorithm.

4.2. Effect of the Network Density

In this set of simulation experiments we vary the number of nodes in the network for a fixed traffic of 12 CBR/s and for a fixed node speed of 12 m/s. We vary the number of nodes in the network and study the average end-to-end delay time, the delivery ratio, and the average power consumption per node per second.

Figures 5-7 show an important improvement on the end-to-end delay, delivery ratio and power consumption of EGBB-AODV compared to AODV and PCB-AODV, especially when the network density increases. **Figure 5** shows that when the network density increases the end-to-end delay of EGBB-AODV remains constant which not the case for AODV and PCB-AODV where both have linear increase. **Figure 6** shows that when the density is high (300 nodes) the delivery ratio of AODV is as very low as 30% and 50% for PCB-AODV but the delivery ratio of EGBB-AODV is still good within 90%. The improvement in the overall performance could be explained by the same reasons as in the previous experiment. Add to it the fact that when the number of node increases the number of rebroadcast of RREQ increases considerably in AODV but the number of rebroadcast in EGBB-AODV is constant (independent from the network density, 8 gateway nodes per hop). This fact is clearly shown in **Figure 7** where the power consumption per node is very low compared to the others. It is almost constant in EGBB-AODV but the power consumption of AODV seems to increase linearly with the number of nodes in the network.

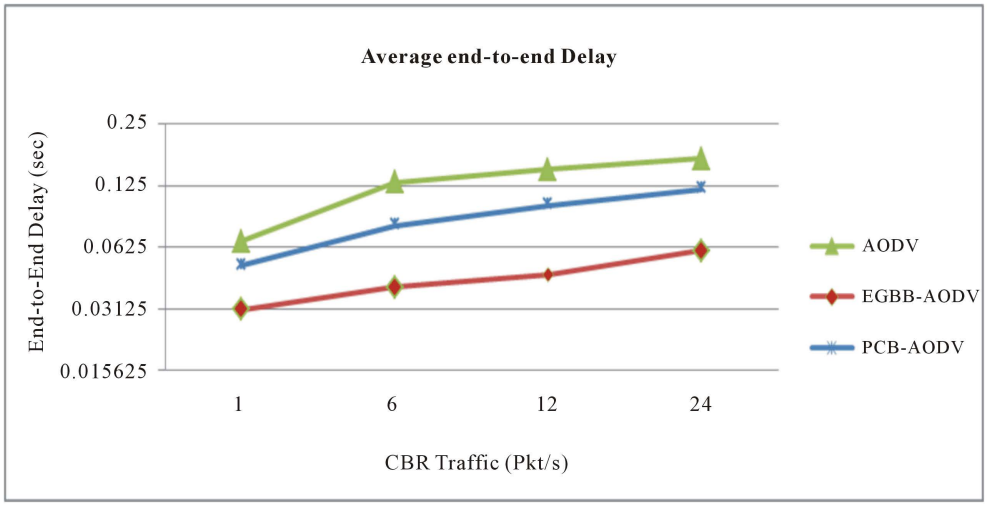


Figure 2. End-to-end delay versus traffic.

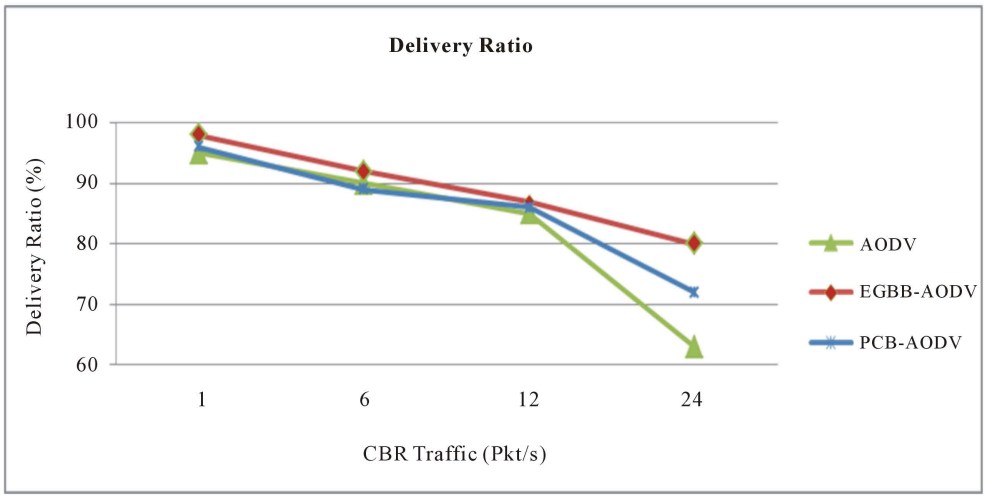


Figure 3. Delivery ratio versus traffic.

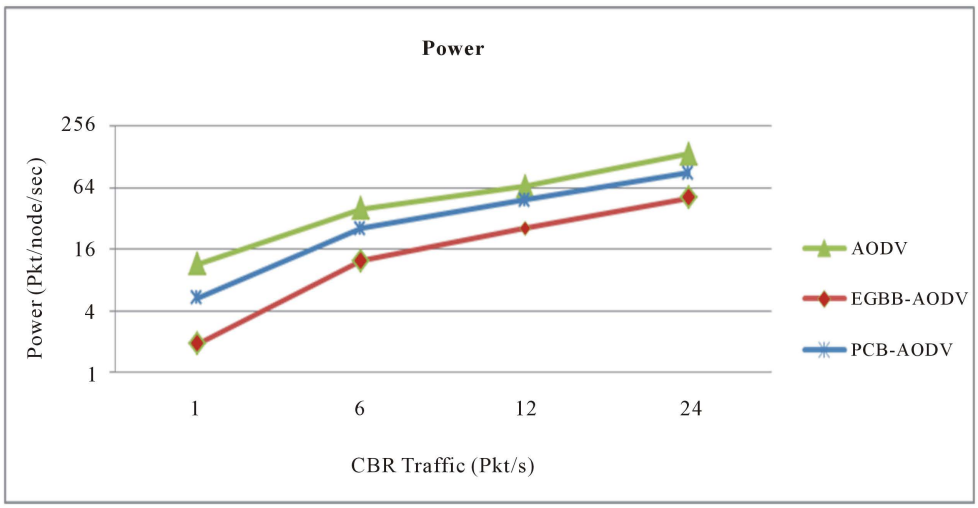


Figure 4. Power versus traffic.

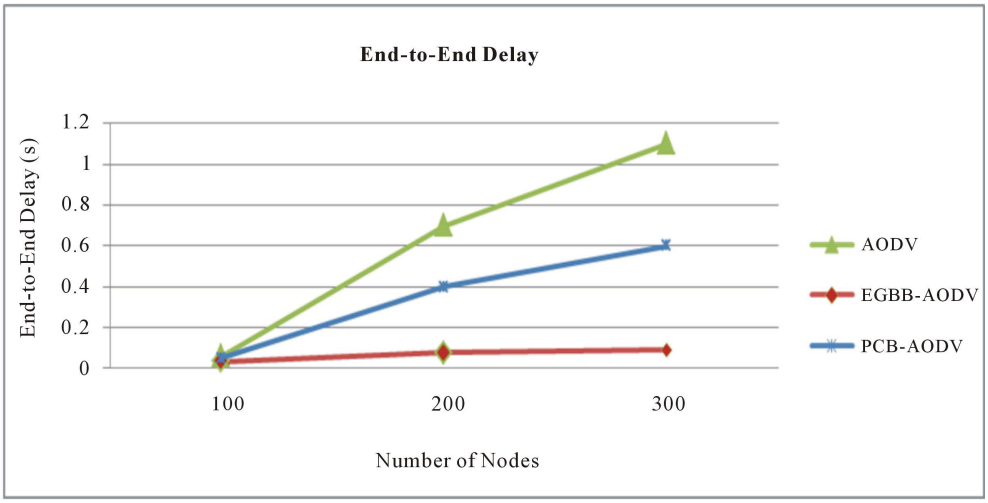


Figure 5. End-to-end delay versus density.

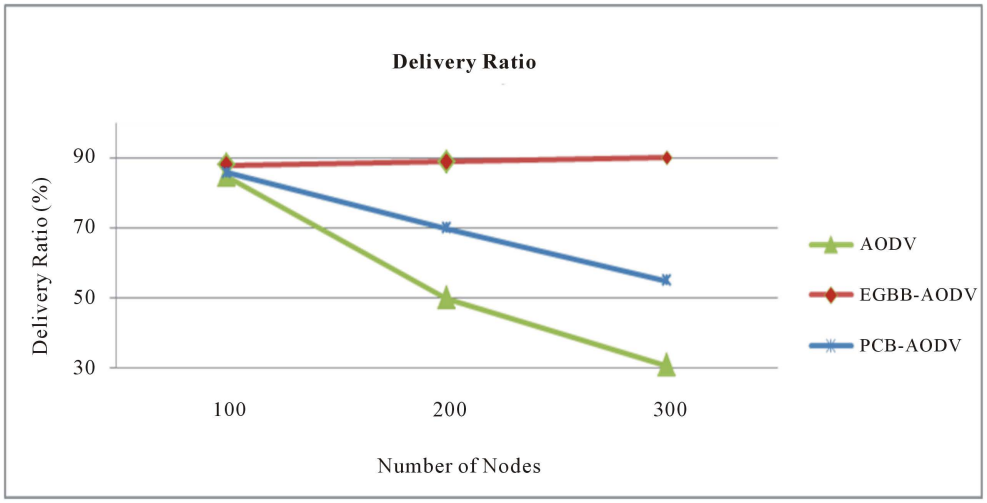


Figure 6. Delivery ratio versus density.

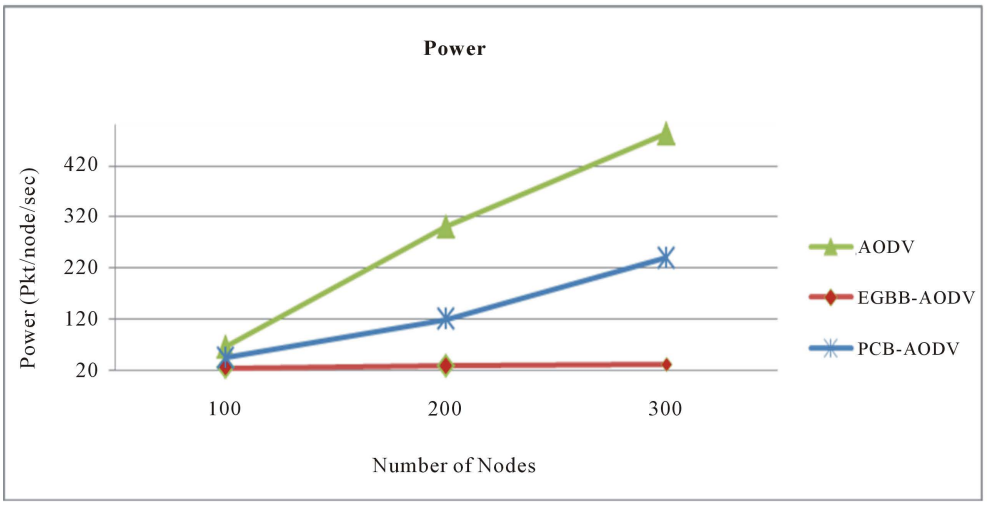


Figure 7. Power consumption versus density.

5. Conclusion

This paper proposed a new modified EGBB-AODV routing protocol for MANET. EGBB-AODV protocol uses a sophisticated broadcast algorithm for sending route request packet RREQ when the original AODV uses a simple flooding to send RREQ. Results obtained from an extensive simulation have revealed a considerably lower end-to-end delay, lower power consumption, and higher delivery ratio of the new protocol EGBB-AODV compared to the traditional AODV and PCB-AODV especially with dense networks. EGBB broadcast algorithm could be applied to enhance the performance of any on-demand routing protocol which uses simple flooding to broadcast the route requests. As a future work, we plan to optimize better the number of rebroadcast in EGBB-AODV to adapt to the traffic density and the nodes mobility to apply it for WSN with high density and low mobility and VANET.

Acknowledgements

This work is funded from Sultan Qaboos University Internal Grant.

References

[1] Murthy, C.S.R. and Manoj, B.S. (2004) Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, New Jersey.

[2] Johnson, D. and Maltz, D. (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski, T. and Korth, H.F., Eds., *Mobile Computing*, Kluwer Academic Publishers, Dordrecht. http://dx.doi.org/10.1007/978-0-585-29603-6_5

[3] Perkins, C. (1997) Ad Hoc on Demand Distance Vector (AODV) Routing. IETF Internet Draft, Work in Progress.

[4] Haas, Z.J. and Pearlman, M.R. (1998) The Zone Routing Protocol (ZRP) for Ad Hoc Networks. Internet Draft, Work in Progress.

[5] Ko, Y.-B. and Vaidya, N.H. (1998) Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. *Proceedings of IEEE/ACM International Conference on Mobile Computing and Networking* (*MOBICOM*), 66-75. http://dx.doi.org/10.1145/288235.288252

[6] Touzene, A. and AlKhathiri, A. (2015) Performance Analysis of an Extended Grid Based Broadcast Algorithm in Mobile Ad-Hoc Networks. *Wireless Networks*, **21**, 659-672. http://dx.doi.org/10.1007/s11276-014-0809-8

[7] Yu, Y. and Yao, Y.B. (2012) Improved AODV Routing Protocol for Wireless Sensor Networks and Implementation Using OPNET. *Third International Conference on Intelligent Control and Information Processing* (*ICICIP*), Dalian, 15-17 July 2012, 709-713. http://dx.doi.org/10.1109/icicip.2012.6391523

[8] Ding, B., Chen, Z.H., Wang, Y. and Yu, H. (2011) An Improved AODV Routing Protocol for VANETs. *International Conference on Wireless Communications and Signal Processing* (*WCSP*), Nanjing, 9-11 November 2011, 1-5. http://dx.doi.org/10.1109/wcsp.2011.6096736

[9] Hafeez, K., Zhao, L., Liao, Z. and Ma, B.N. (2010) A New Broadcast Protocol for Vehicular Ad Hoc Networks Safety Applications. *Proceedings of the IEEE Conference on Global Telecommunications*, Miami, 6-10 December 2010, 1-5. http://dx.doi.org/10.1109/glocom.2010.5683409

[10] Harutyunyan, H. and Wang, W. (2010) Broadcasting Algorithm via Shortest Paths. *Proceedings of the IEEE* 16*th International Conference on Parallel and Distributed Systems*, Shanghai, 8-10 December 2010, 299-305. http://dx.doi.org/10.1109/icpads.2010.110

[11] Gandhi, R., Kim, Y.A., Lee, S., Ryu, J. and Wan, P.J. (2012) Approximation Algorithms for Data Broadcast in Wireless Networks. *IEEE Transactions on Mobile Computing*, **11**, 1237-1248. http://dx.doi.org/10.1109/TMC.2011.162

[12] Khabbazian, M., Blake, I.F. and Bhargava, V.K. (2012) Local Broadcast Algorithms in Wireless Ad Hoc Networks: Reducing the Number of Transmissions. *IEEE Transactions on Mobile Computing*, **11**, 402-413. http://dx.doi.org/10.1109/TMC.2011.67

[13] Medetov, S., Bakhouya, M., Gaber, J. and Wack, M. (2013) Evaluation of an Energy-Efficient Broadcast Protocol in Mobile Ad Hoc Networks. *Proceedings of the* 20*th International Conference on Telecommunications* (*ICT*), Casablanca, 6-8 May 2013, 1-5. http://dx.doi.org/10.1109/ictel.2013.6632108

[14] Zhang, X.M., Wang, E.B., Xia, J.J. and Sung, D.K. (2013) A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, **12**, 424-433.

[15] Ahmadi, A., Shojafar, M., Hajeforosh, S., Dehghan, M. and Singhal, M. (2014) An Efficient Routing Algorithm to Preserve *k*-Coverage in Wireless Sensor Networks. *The Journal of Supercomputing*, **69**, 599-623.

http://dx.doi.org/10.1007/s11227-013-1054-0

[16] Xiong, H. and Bodanese, E. (2011) A Signal Strength Based Medium Access Control for OFDMA Based Wireless Ad Hoc Networks. *Proceedings of the* 18*th International Conference on Telecommunications*, Ayia Napa, 8-11 May 2011, 439-443. http://dx.doi.org/10.1109/CTS.2011.5898965

[17] Obaidat, M., Ali, M.A., Obaidat, M.S., Obeidat, S. and Shahwan, I. (2011) A Novel Multipath Routing Protocol for MANETs. *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, 23-25 September 2011, 1-6. http://dx.doi.org/10.1109/wicom.2011.6040394

[18] Stojmenovic, I. (2002) Position-Based Routing in Ad Hoc Networks. *IEEE Communications Magazine*, **40**, 128-134.

[19] Giordano, S., Stojmenovic, I. and Blazevic, L. (2003) Position Based Routing Algorithms for Ad Hoc Networks: A Taxonomy. In: Cheng, X., Huang, X. and Du, D., Eds., *Ad Hoc Wireless Networking*, Kluwer Academic Publishers, Boston.

[20] Mauve, M., Widmer, J. and Hartenstein, H. (2001) A Survey on Position-Based Routing in Mobile Ad-Hoc Networks. *IEEE Network Magazine*, **15**, 30-39. http://dx.doi.org/10.1109/65.967595

[21] Kamali, S. and Opatrny, J. (2008) POSANT: A Position Based Ant Colony Routing Algorithm for Mobile Ad Hoc Networks. *Journal of Networks*, **3**, 31-41. http://dx.doi.org/10.4304/jnw.3.4.31-41

[22] Endo, K., Inoue, Y. and Takahashi, Y. (2012) Performance Modeling of Beaconless Forwarding Strategies in Multi-Hop Wireless Networks. *Computer Communications*, **35**, 120-128. http://dx.doi.org/10.1016/j.comcom.2011.08.001

[23] Hightower, J. and Borriello, G. (2001) Location Systems for Ubiquitous Computing. *Computer*, **34**, 57-66. http://dx.doi.org/10.1109/2.940014

[24] Wu, X., Yang, Y., Liu, J., Wu, Y. and Yi, F. (2010) Position-Aware Counter-Based Broadcast for Mobile Ad Hoc Networks. *Proceedings of the* 2010 *Fifth International Conference on Frontier of Computer Science and Technology* (*FCST*), Changchun, 18-22 August 2010, 366-369.

[25] Fadah, A., Lawati, A., AlMaskari, S., Touzene, A. and AlKindi, A. (2008) Experimental Evaluation of Wireless IEEE802.11b Networks. *Proceedings of the First International IEEE Conference on Application of Digital Information on Web Technologies* (*ICADIWT*2008), Ostrava, 4-6 August 2008.

[26] Chinara, S. and Rath, S.K. (2009) A Survey on One-Hop Clustering Algorithms in Mobile Ad Hoc Networks. *Journal of Network System Management*, **17**, 183-207. http://dx.doi.org/10.1007/s10922-009-9123-7

[27] Lucent Technologies (1999) WaveLan IEEE 802.11 PC Card User's Guide. http://www.wavelan.com

[28] IEEE Standard 802.11 (1997) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[29] Boudec, J.Y.L. and Vojnovic, M. (2005) Perfect Simulation and Stationarity of a Class of Mobility Models. *Proceedings of the IEEE INFOCOM*, **4**, 2743-2754. http://dx.doi.org/10.1109/infcom.2005.1498557

Int. J. Communications, Network and System Sciences, 2015, 8, 533-542
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813048

Scientific Research Publishing

Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite

Şadan Cambazoglu[1], Arif Sari[2]

[1]Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
[2]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: sdn1991@gmail.com, arifsari@gau.edu.tr

Received 3 July 2015; accepted 27 December 2015; published 30 December 2015

Abstract

Jamming attack is quite serious threat for Mobile networks that collapses all necessary communication infrastructure. Since mobile nodes in Mobile Ad Hoc Networks (MANET) communicate in a multi-hop mode, there is always a possibility for an intruder to launch a jamming attack in order to intercept communication among communication nodes. In this study, a network simulation has been carried out in order to explore and evaluate the possible impacts of jamming attack on MACAW protocol. Ad-hoc network modelling is used to provide communication infrastructure among mobile nodes in order to modelling the simulation scenarios. In simulation model, these nodes have used AODV routing protocol which is designed for MANET while second scenario contains simulated MACAW node models for comparison. On the other hand, this paper is the first study that addresses performance evaluation of MACAW protocol under a constant Jamming Attack. The performance of MACAW protocol is simulated through OPNET Modeler 14.5 software.

Keywords

OPNET, Simulation, MACAW, Mobile Ad-Hoc Networks, Collision, Jamming, AODV

1. Introduction

Wireless networks take important place in the world of communication. Today a great number of people such as businessmen, managers, students and employees can easily access to the internet or to the corporate networks through wireless connections. Although wireless technologies expand the limits of communication area, they are exposed to some problems due to their nature. These problems violate quality of wireless communication.

How to cite this paper: Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. *Int. J. Communications, Network and System Sciences*, **8**, 533-542.
http://dx.doi.org/10.4236/ijcns.2015.813048

Collision, one of these problems occurs when two nodes in the same network, attempt to transmit data at the exact same time [1]-[4]. Corresponding problem results in loss of quality in communication. Especially in mobile wireless networks collision avoidance issue becomes more difficult due to transmission environment. Up to now, considerable solutions addressing to this problem have been proposed in variety of researches.

MACAW, one of these solutions provides effective collision avoidance mechanisms. MACAW protocol is generally used in mobile wireless networks [4]-[6].

On the other hand, security attacks which are another reason for collision occurrence, result in loss of quality in communication as well. In this study, a network simulation has been carried out in order to evaluate performance of MACAW protocol. During this simulation, MACAW protocol has been exposed to a constant Jamming Attack which results high collision occurrence rate in the network. The entire network mechanisms are simulated through OPNET Modeler 14.5 simulation software which is widely used in the network industry to estimate behaviors of network component in a virtual environment. The importance of this study is the first simulation case that addresses performance evaluation of MACAW protocol under a Jamming Attack.

2. Collision in Mobile Wireless Networks

In computer networks, there are many nodes and they have to transmit data packages over the same carrier. This carrier can be an optic cable in wired networks while it is a frequency in wireless networks. Owing to this networking principle, if two nodes in the same network attempt to send data packages to the communication line at the exact same time, a collision occurs. Collisions are important problems for networks because they violate data transmission and results in loss of information. When any collision occurs in the network, the communication stops; ultimately, data packages are dropped. Collisions always results in less throughput of the network, high network load, high delay and high data drop rate [7]-[9].

2.1. Collision Avoidance Protocol in Mobile Wireless Networks

As mentioned previously, owing to collisions, network nodes face with loss of packet integrity. That means a proper communication cannot be established in the network. In seven layer OSI model [10]-[12], Media Access Control (MAC) layer is responsible for avoidance of package collision. MAC sub layer performs this task through avoidance protocols. These protocols play a critical role in preventing data collision; they aim to rule situations out which multiple nodes access to the network at the exact same time and to provide packet transmission to any node without any collision. There are some protocols that mostly used and are developed to prevent collisions in the networks such as ALOHA, CSMA, MACA and MACAW.

MACAW Protocol

Multiple Access with Collision Avoidance for Wireless (MACAW) is a widely used MAC sub layer protocol. MACAW is useful for mobile ad-hoc networks. It contains new collision avoidance mechanisms. By these mechanisms data transmission is completed in five steps. These five steps are Request-to-Send (RTS), Clear-to-Send (CTS), Data Sending (DS), data packages and Acknowledgement (ACK). RTS is a message, sent from data sender node to receiver node, notifies that a node attempts to transmit data to another node. CTS message is a respond for transmission request. If receiver node available for transmission then sends a CTS message. DS frame informs receiver node about the size of data package. After that, data transmission starts. When it completes properly, receiver node sends an ACK message to sender node. ACK notifies that data transmission completed successfully [13]-[16].

3. Network Simulation

In computer networking field, testing a complete network's behaviors in a real environment is a quite costly process. In this case network simulation techniques provide an opportunity to test network equipment such as routers, servers and cables in an inexpensive way. Besides that, network protocols, networks services and other network features can be tested to see behaviors of nodes. Network simulation actions are performed by network simulators in a virtual environment. A network simulator is a software application that estimates behaviors of nodes, equipment and protocols of a modelled network. Simulators typically support commonly used networking technologies such as Wi-Max, WLAN, and ZigBee. Most of these simulators have a Graphical User Inter-

face (GUI). As well as GUI simulators, Command Line Interface (CLI) simulators are also available. Some network simulation software are open source while some are proprietary software. Commonly used simulators are GNS3, ns, OPNET, NetSim, OMNeT++ [17] [18].

3.1. Simulated Node Models

In this simulation experiment while evaluating collision effects on network, mobile nodes have been used. These mobile nodes create an ad-hoc network among them. In OPNET simulator these types of nodes are called as "manet_station_adv". While simulating scenario, 50 nodes were used.

3.2. Simulation Model and Experiment Environment

While performing simulation scenarios, OPNET Modeler 14.5 has been used. In this simulation, 2 different scenarios are designed. The simulation was performed in a 1000 × 1000 meters campus area with 50 mobile nodes. These nodes share the common parameter attributes. In **Table 1**, all global simulation parameters are shown in detail.

In this simulation model, MACAW and AODV protocols are used. The performance evaluation and contents of the protocol is exposed by the researchers in the literature before [19] [20]. MACAW as mentioned before, is a powerful collision avoidance protocol and used in this simulation model for its specific purpose. On the other hand Ad hoc On-Demand Distance Vector (AODV) [2] is a routing protocol that is used in mobile ad-hoc networks while nodes determining their destination paths for data transmission. Simulation has been carried out for 1 hour in a 1000 × 1000 meters area, Mobility Model status was stated as Simple Random Waypoint with constant speed of 10 meter/seconds. Network Throughput, Network Load and Delay parameters are taken as Performance Parameters. Data Rate was set as 11 Mbps which is maximum data rate for IEEE 802.11 b. Trajectory

Table 1. Simulation scenario parameters.

Parameters	Attributes
Protocols	MACAW-AODV
Simulation Time	1 Hour
Simulation Area	1000 × 1000 (meters)
Mobility Model	Simple Random Waypoint
Mobility m/s	1/10
Performance Parameters	Throughput, Network Load, Delay, Drop Rate
Transmit Power (W)	0.005
RTS Threshold (bytes)	1024
Data Rate (Mbps)	11 Mbps
Pkt. Reception power Threshold	−95 dbm
Buffer Size	1024,000
Pkt. Size (bits)	2000
Pkt. Interarrival time (seconds)	0.03
Trajectory	VECTOR
Start time (seconds)	10
End Time	End of Simulation
No of Seeds	40,000

was set as Vector which means mobile nodes change their location unsymmetrically. Finally, Seed value which is number of network events performed in 1 second, was set as 40,000. The successful simulation scenarios have been conducted on simulated different contention-based or contention-less protocols through OPNET in the literature [19] [20]. So it is quite reliable to conduct this simulation scenario through OPNET simulation package.

3.2.1. Simulation Scenario 1

In the first scenario, there are 50 mobile nodes that have an ad-hoc network among them. They move at a constant speed of 10 meters per second. **Figure 1** below illustrates these nodes distributed randomly in a 1000 × 1000 meters area.

In this scenario illustrated, Application profile, Profile configuration and Mobility configuration are defined to meet network requirements specified in **Table 1**. Network model has two scenarios. In first scenario, nodes communicate with each other in a proper way. There is no malicious node and no security attack. One of these nodes acts as an Access Point at the same time. OPNET simulator has evaluated this scenario for 1 hour. Simulation results were measured and evaluated according to network performance metrics. The main purpose for this scenario is to determine status of network under normal conditions. This scenario will be useful while comparing effects of collisions and security attacks to network performance.

3.2.2. Simulation Scenario 2

In this scenario again 50 mobile nodes have been used. Unlike Scenario 1, here also 3 mobile jammer nodes have been used. Scenario 2 is shown on the **Figure 2**.

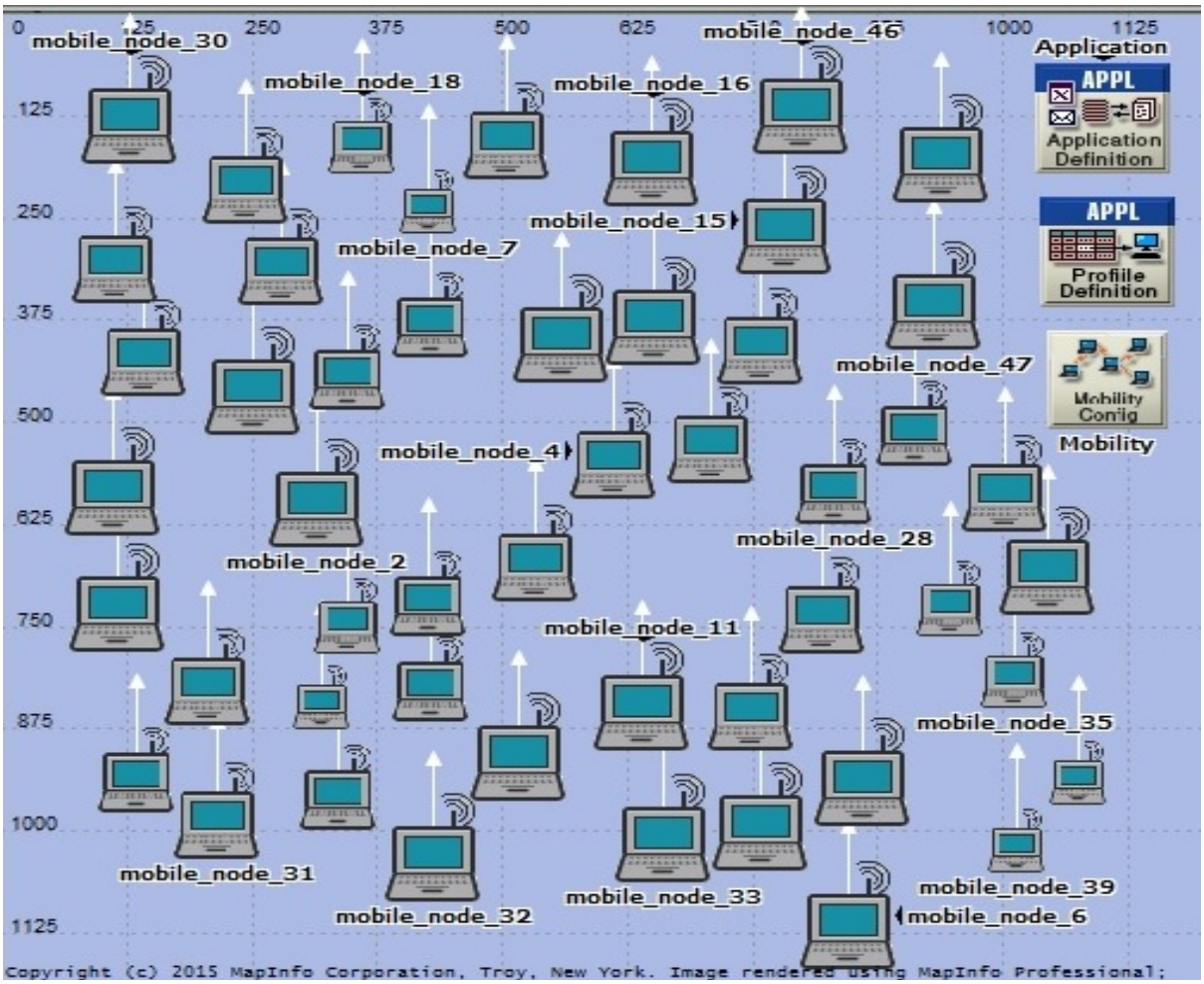


Figure 1. Simulation Scenario 1.

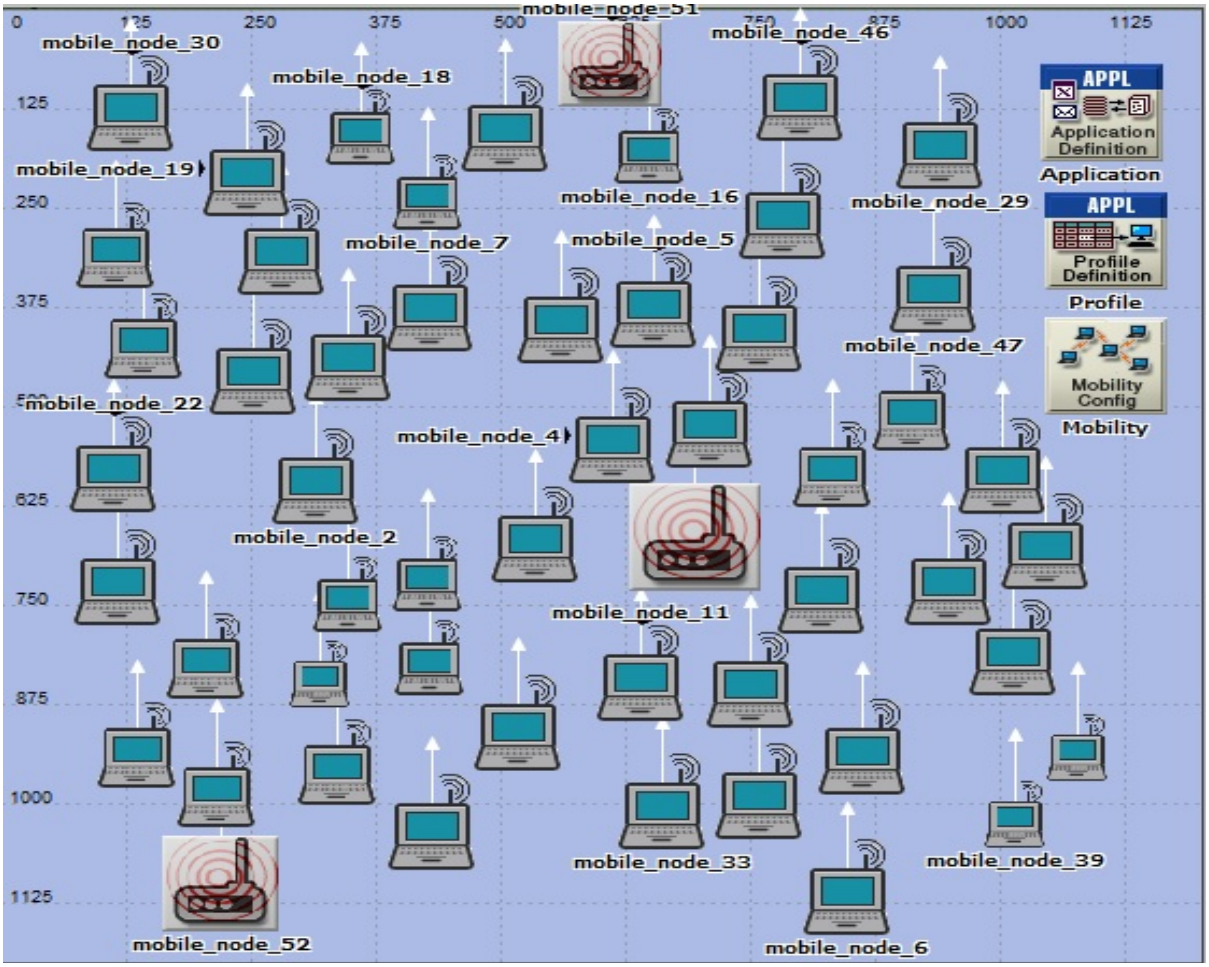


Figure 2. Simulation Scenario 2.

While these nodes attempting to communicate between each other properly, two jammer nodes violate communication. They constantly sent large size data packages to the network so that it causes less network throughput, collision occurrences and high network traffic. These jammer nodes were specified according to requirements of the project. Jammer nodes transmit data packages in large sizes. It sends constantly 10,000 bits size of data packages. In simulation model this jamming attack will keep being as long as the simulation continue. Therefore network communication is affected adversely.

All these circumstances directly affect network throughput. In scenario 2, these conditions have been simulated and evaluated. Comparison results of two scenarios clearly show how jamming attacks cause less throughput and high collision occurrence.

3.3. Performance Metrics

Simulation results are evaluated according to determined network performance criteria. In this experiment four performance metrics are taken. These metrics are Network Throughput, Network Load, WLAN Delay and Data Dropped. The network throughput refers to the amount of bits forwarded successfully from one network layer to another in a given time. Network throughput is typically measured as bits per second (bps), megabits in per second (Mbps) and gigabits per second (Gbps). On the other hand, Network Load is described as measurement of total data traffic on a WLAN Base Station Subsystem (BSS). It shows BSS load statistics of a network separately. Other performance metric which is WLAN Delay, represents latency of packages while they are travelling from one device to another. Finally Data Dropped statistics show total amount of data packages that are discarded by higher network level due to high buffer size of packages.

4. Simulation Results

Two scenarios have been subjected to simulation for one hour. In first scenario 50 mobile nodes had a proper communication between each other. There were not any malicious nodes or security attacks. These nodes have used MACAW protocol as collision avoidance protocol as well as they have used AODV protocol as mobile ad-hoc network routing protocol. Likewise scenario 1, scenario 2 had the same protocols, and equal number of mobile nodes. On the other hand unlike scenario 1, scenario 2 had also 3 mobile constant jammer nodes. Network model in scenario 2 was exposed to a powerful and constant jamming attack. These jammer nodes have sent large data packages to the network. In simulation results we have seen the performance of MACAW protocol under jamming attack condition. These 2 scenarios were simulated within a Discrete Event Simulation (DES) environment. Simulation outcomes and statistics were generated by OPNET Modeler 14.5 in graphical charts according to mentioned conditions.

4.1. Average WLAN Throughput Statistics

As stated before, Network Throughput refers to number of bits that are forwarded successfully one layer to another in a given time. Measurement for this statistics is used to be bits per second (bps). In this topic, two scenarios' throughput is compared to each other. It is expected that throughput of scenario 1 would be higher than scenario 2 because as mentioned in previous chapters, malicious nodes and security attacks directly affect overall network performance. OPNET Modeler 14.5 has provided throughput comparison of the two scenarios as a consequence of 1 hour simulation. In the following figure, WLAN Throughput statistics comparison of 2 scenarios is shown.

Figure 3 clearly illustrates average Wireless LAN Throughput comparison of two scenarios. In the first scenario which doesn't have any malicious nodes, it can be easily seen that bit transfer rate is above 8,000,000 bits per second. Under normal network conditions network throughput reaches up to approximately 7.7 Mbit. Second scenario which is represented by a red line in the figure shows that when network is exposed to a jamming attack its overall throughput rapidly decreased below 3000,000 bits per second. It can be clearly seen that jamming attack has a significant impact on overall network performance. It decreases throughput approximately three times.

4.2. Average Wireless LAN Delay Statistics

Wireless LAN Delay statistics represent package latency while they are transferring one layer to another. When network performance is low, package transmission slows down. In this case total network delay becomes high. In **Figure 4**, comparison graphics of scenarios for Wireless LAN Delay statistics can be seen.

Blue line which represents Scenario 1 shows that WLAN Delay rate is close to zero seconds. In normal network state, packages are delivered one layer to another without more delay. However in second scenario it can be seen that package delay have rapidly increased. Jamming attack caused a significant latency of packages.

4.3. Average Wireless Data Dropped Statistics

As discussed previously, data drop rate represents data packages that are discarded by higher level network layer. When buffer size of a data package is higher than determined acceptable value, network automatically drops the data package. As known, in Denial of Service attacks malicious nodes constantly send packages in large sizes to make network resources unavailable. As measure, network administrators adjust server nodes to drop these large size data packages. In simulation scenarios, "Large Packet Processing" option is set as "Drop" in order to protect the network against possible damages of large size packages. Below **Figure 5** shows average Wireless LAN Data Dropped statistics.

Figure 5 clearly shows data drop rate comparisons of two scenarios. As seen, red line which represents Scenario 2 is higher than blue line. Because jammer nodes send packages in 10,000 bits size and network directly drops them.

4.4. Average Wireless LAN Network Load Statistics

Network Load represents measurement of total amount of data over entire network. In **Figure 6** Wireless LAN Network Load statistics comparison of two scenarios is shown.

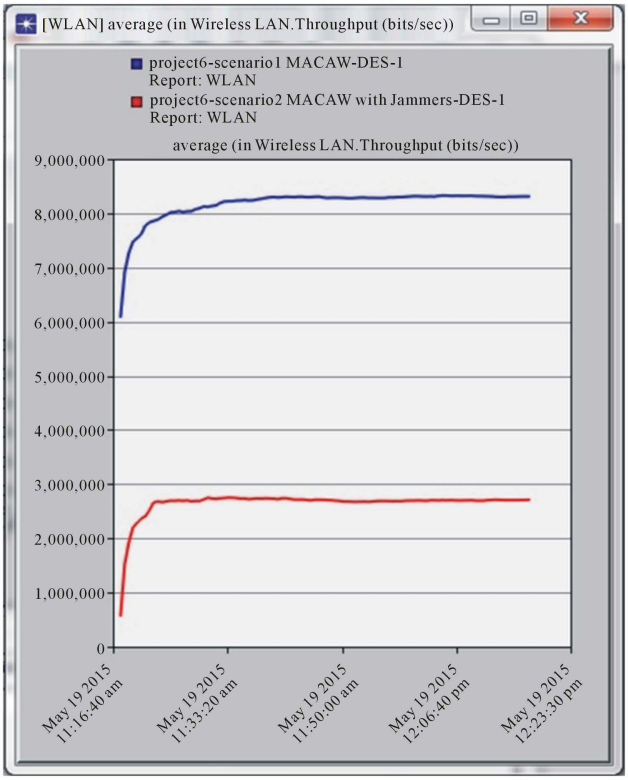


Figure 3. Average WLAN throughput comparison.

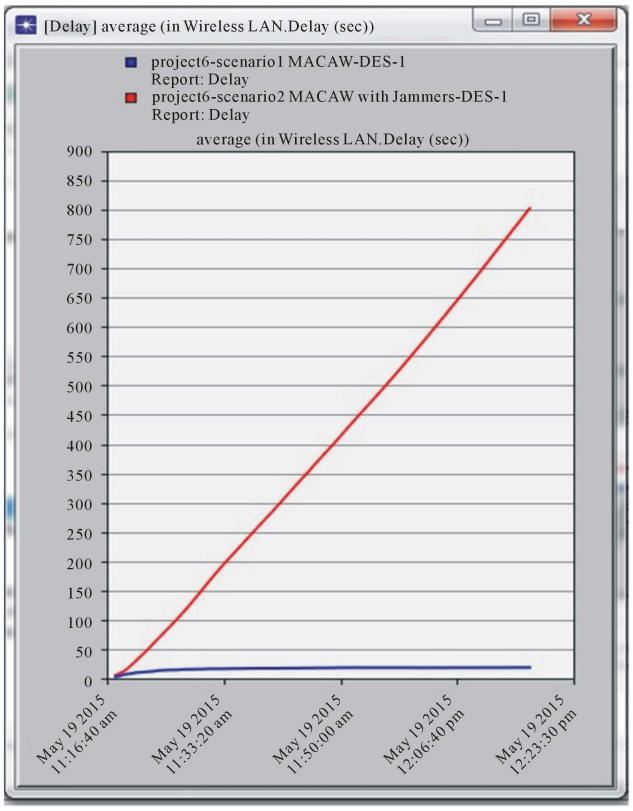


Figure 4. Average WLAN delay statistics.

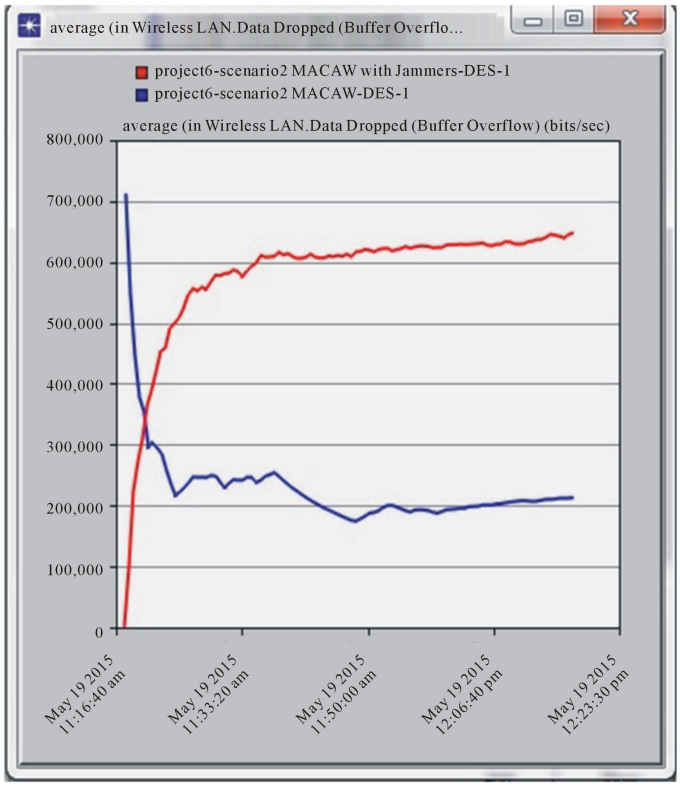


Figure 5. Average WLAN data dropped statistics.

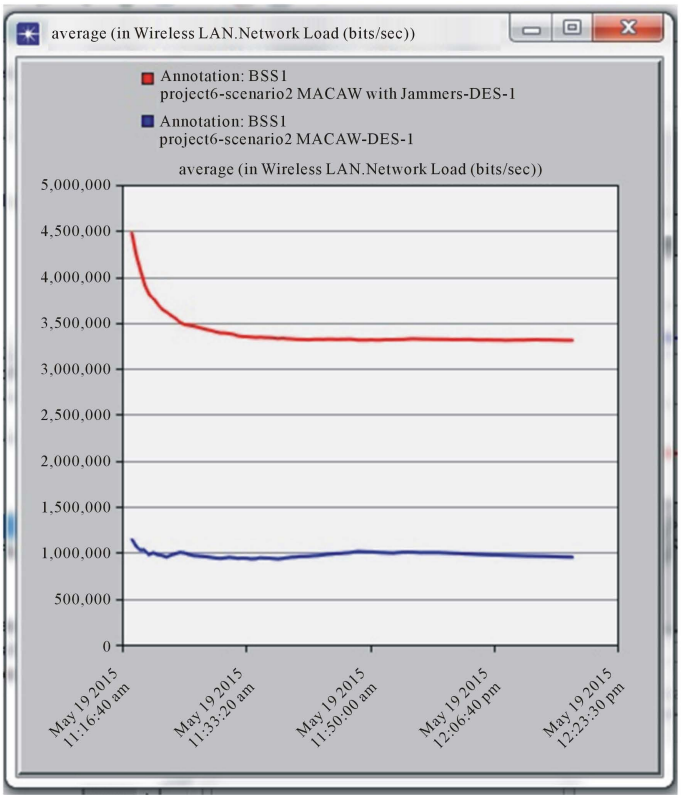


Figure 6. Average WLAN network load.

As it is shown through direct relationship between the average WLAN Data Dropped Rate on **Figure 5** and average WLAN Network Load on **Figure 6**, the scenario 2 had higher data dropped rate due to jamming attack and network load shown on **Figure 6** is higher due to injected packages into network through jammers. The huge amount of injected packages dropped from the network that is proven by the **Figure 5** with higher data dropped rate of scenario 2 and high network load value of **Figure 6** for scenario 2.

5. Conclusion

In the simulation case of study, the performance of MACAW protocol is evaluated. During this simulation, MACAW protocol has been exposed to a constant Jamming Attack. The main goal of this study is to observe possible impacts of a constant Jamming Attack on MACAW protocol. MACAW has shown a good performance unless it has been exposed to a Jamming Attack. It is seen in the simulation results that, a Jamming Attack in a mobile ad-hoc network leads to loss of performance of MACAW. Based on the simulation results, it can be claimed that Jamming Attacks cause approximately three times loss of network throughput where MACAW protocol is implemented. Delay rate in the network has significantly increased up to 800 seconds during Jamming Attack while it is close to zero second under normal network conditions. On the other hand, Data Dropped statistics show that 600,000 packages are discarded when MACAW is exposed to attack. In normal network conditions, this statistics is stable at the rate of 200,000 dropped data packages. In the jamming scenario, Network Load which is the final performance criteria shows that average load is at the rate of 4500,000 bits per second in the beginning of the simulation whereas it is stable at approximately 3500,000 bits per second at the end of the simulation. However, in the normal scenario Network Load statistics is stable at the rate of 1000,000 bits per second. Jamming Attack causes not only three times decrease in the network throughput but it also causes three times increase in the network load. This simulation experiment is the first study that deals with the performance evaluation of MACAW protocol under a constant Jamming Attack. Depending on results of our simulation experiment, it is strongly recommended other researchers to simulate performance of MACAW protocol under different security attacks such as Man in the Middle, Distributed Denial of Service and Spoof Attack. It is also recommended that precautions against attacks should be taken in MACAW protocol.

References

[1] Rouse, M. Collision Definition. http://searchnetworking.techtarget.com/definition/collision

[2] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[3] Sharanappa, P.H. and Mahabaleshwar, S.K. (2014) Performance Analysis of CSMA, MACA and MACAW Protocols for VANETs. *International Journal of Future Computer and Communication*, **3**.

[4] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[5] Joa-Ng, M. (1999) Spread Spectrum Medium Access Protocol with Collision Avoidance in Mobile Ad-hoc Wireless Network. *INFOCOM*'99, *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, **2**. http://dx.doi.org/10.1109/infcom.1999.751465

[6] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94.

[7] Zimmermann, H. (1980) OSI Reference Model—The IS0 Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, **COM-28**, 425-432. http://dx.doi.org/10.1109/TCOM.1980.1094702

[8] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372.

[9] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education, United Kingdom*, **2**, 1-6.

[10] Bharghavan, V., Demers, A., Shenker, S. and Zhang, L. (1994) MACAW: A Media Access Protocol for Wireless LAN's.

[11] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence, United Kingdom*, **2**, 11-18.

[12] Pan, J. (2008) A Survey of Network Simulation Tools: Current Status and Future Developments. http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf

[13] Sari, A. (2015) Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, Hershey, 66-94. http://dx.doi.org/10.4018/978-1-4666-8345-7.ch005

[14] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[15] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[16] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[17] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN*'13), ACM, New York, 454-456. http://dx.doi.org/10.1145/2523514.2523586

[18] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 *Fifth International Conference on Computational Intelligence, Communication Systems and Networks* (*CICSyN*), 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[19] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), 9-11 May 2013, 579-582.

[20] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

Int. J. Communications, Network and System Sciences, 2015, 8, 543-551
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813049

Scientific Research Publishing

Dissemination of Information Communication Technologies: Mobile Government Practices in Developing States

Mustafa Bal[1], Cem Gonenc Biricik[1], Arif Sari[2]

[1]Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
[2]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: mustafabal93@hotmail.com, gonencbiricik@gmail.com, arifsari@gau.edu.tr

Received 11 February 2015; accepted 27 December 2015; published 30 December 2015

Abstract

Information Communication Technologies (ICT) has offered m-government applications as an intermediate technology to provide effective and efficient government services to the public. Due to high rate of corruptions in developing states, government policies diversified governmental services from offline to virtualized perspective to expose accessibility, transparency, accountability and accessibility through mobile government. Deployment of such ICT tool also exposed a unique opportunity for the recovery of the public confidence against government which has damaged due to corruption activities in country. Virtualization of the government services became compulsory due to high rate of corruption that occurred in the economic context and it became a serious obstacle for economic development of developing states. The virtualized services aimed to harmonize governmental services into mobile platform in order to become more transparent to the public. This research paper comparatively investigates the mobile government services that are located in Malta and Singapore which are classified as developing countries. The criteria of the comparison have done based on demographic structure of the country, M-government policies and ICT infrastructure of the country. The findings of this study exposed the impact of e-government practices and differences between them in terms of applicability and provide a specific point of view for m-government adoption policy.

Keywords

M-Government, Developing States, Virtualization, ICT, Policy, Malta, Singapore

How to cite this paper: Bal, M., Biricik, C.G. and Sari, A. (2015) Dissemination of Information Communication Technologies: Mobile Government Practices in Developing States. *Int. J. Communications, Network and System Sciences*, **8**, 543-551.
http://dx.doi.org/10.4236/ijcns.2015.813049

1. Introduction

Nowadays, mobile government applications developed to provide service to citizens of developed and developing countries more efficiently, effectively and quickly. E-government applications of information and communication technologies in a guided way to mobilize the services offered to the citizens are the simplest definition of the mobile government. The spread usage of mobile services forced new transition of e-government services inevitably to mobility [1]-[4]. In today's world that globalizing, science and technology more accelerated day by day, ICT is now being leverage for other sectors ceased to be a branch of technology [3]-[5]. Basic ICT infrastructure of developing states countries such as Singapore and Malta are investigated to expose current state of mobile government in Malta, its effectiveness and efficiency, usage and assess the overall mobile government strategy. ICT is one of the indispensable elements of life in economic and social life. Variety of country uses ICT in the public sector more consistently, tended to structure offering cheap and accurate services where this structure is defined as e-government. Most important in the country's service sector is among the reasons for the importance of mobile research and development had given the state administration, the country's population density varies in importance given to the technology of the population and by the country of service. In this article, the mobile application of the two island nations government, unlike other countries, to draw attention to the importance it attaches to research and development has been requested. As little more than the population of the Maltese government had to the need for research and development of the Maltese island country wants to develop the smart vision and need for appropriate research and development of the later start of the state of the mobile government applications development within singapore government has taken care to provide more slowly by the Maltese government and development. Using technological possibilities of access to ICT and public services citizens in this way to get more efficient and higher quality services indicate a need beyond necessity. ICT are closer to the state government to ensure citizens facilitate knowledge management [6]-[8]. Today the development of smart phones is leaded the possibility of access to these services 24/7 through M-government concept. Through the streamlined infrastructure used by M-government structure, E-government services provide anytime access of citizens. In order to create specific attention and desire on m-government, mobile applications are crucially important. To expose a state of m-government applications and the interest-awareness of the citizens, fast, flexible and evolving mobile applications compatible with country's internet and mobile communication infrastructure is compulsory. The research also highlights the state of the m-government resources that these countries have and devoted to provide m-government services in country.

ICT is one of the indispensable elements of life in economic and social life. World using ICT in the public sector more consistent, tended to structure offering cheap and accurate service. This structure is defined as e-government. Using technological possibilities of access to ICT and public services citizens in this way to get more efficient and higher quality services indicate a need beyond necessity. ICT are closer to the state government to ensure citizens facilitate knowledge management [8]-[10]. Today has led the development of smart phones and the people that develop quickly turned to the state and to turn to smartphone applications to access tivity in terms of sectors. M-government, e-government anytime access of citizens created using streamlined infrastructure has to be provided. To develop a state of m-government applications and the interest in it to the citizens to make continuous mobile application and the information is easy to develop applications, to be fast and flexible, evolving according to the country's internet and mobile communication infrastructure. The amount of the state of the resources they devote to providing the importance of m-government applications development.

2. ICT in Developing States

Information Communication Technologies (ICT), which combines computer and communication technologies, information constituting any kind of printed and written information that is accessible by others and visual tools [11]. The vital importance of ICT is to make people's life easier through technological innovations. ICT industry evolved variety of techniques in terms of closing the gap between developing countries and developed countries [12] [13]. ICT is used with the aims towards developing state of the social and economic objectives and can be used as the key to achieve of the state strategy goals. Developing states are able to implement ICT to the most of sectors such as governance, business and education. In order to achieve such goal, country communication infrastructure must be developed and ready to adopt ICT innovations which are quite difficult for developing regions in the world.

3. M-Government

E-Government: Using the state's duty is to fulfill against citizens and services with citizens, state that the duties and responsibilities of the electronic communications and computing environments in a continuous and safe execution of the M state experienced in the real-life state for more efficient operation of e-government in terms of accessibility wireless internet infrastructure mobile applications are moving to laptops [14] [15]. The development of service models is shown on the **Figure 1** below.

Mobile government is a state of providing all e-government services to public through mobile environment with the advantage of the mobile technology. The rapid changes in technological innovations and impact of the Internet forced e-government state to be changed and spread into mobile environment [17].

The successful adoption of the Mobile Government is possible through designing an M-government applications to have an easy access, functional and non-complex interface for the citizens. The digital government strategy is also defined by US and basic conceptual model is designed by considering different principles [17]-[19]. While designing of mobile government applications, it must be user-centered design and ubiquitous, efficient, transparent and innovative.

3.1. M-Government in Developing States

The spread of ICT all around the world lead many opportunities and practical solutions to improve the utilization of resources in developing states. As a result of technological innovations on public services and quality, the cost of services significantly decreased.

Governments have proposed e-government services in mobile platforms after exposing the demand of mobility and necessity of dissemination in e-services in countrywide. Applications derived from e-government in mobile platform have also been supporter for government services where an application illustrates the importance of ease of use and anytime access. Developing countries needs to mobile government. Governments enable country's citizens to engage with an increasingly mobile workforce to access high-quality mobile government services at anywhere, anytime and on any device [20]-[22]. Today, e-government services provide information related with technology, public safety, health, accommodation and emergency.

3.2. M-Government Policies

Government must be able to provide uninterrupted information services to public with quality and provide sustainable information participation of citizen's with engagement of mobile government applications. Mobile

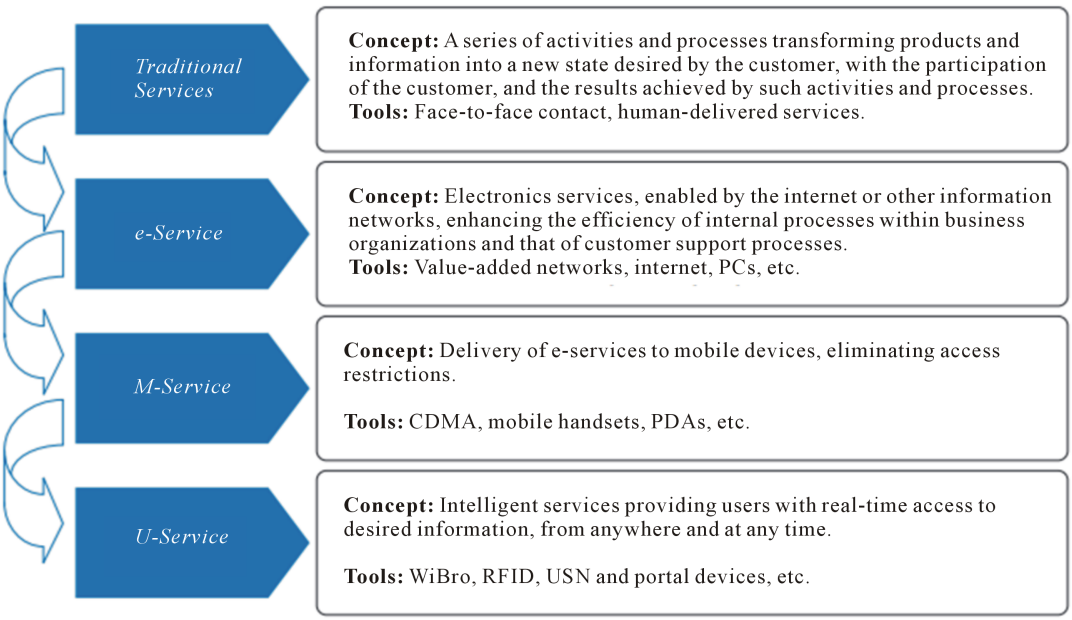


Figure 1. Development of service concepts [16].

devices allow users to conduct convenient operation and 24 hours effectively-sustainable information sharing through e-government applications. Today, citizen monitoring applications and services used by national government to facilitate the collection of statistics and operations of the state, public services and information about the public. Additionally, Mobile Applications used to track of citizens tax payments and legal transactions resulting in the reduction of transaction of paper [23].

4. M-Government in Malta (Institutions, Development and Strategies)

A Malta has started Mobile government applications and virtualization from 2002 to the applications they are developing, especially since citizen-centered paradigm and in line with the mission.

The small population of the Maltese government, Information and resources that it allocates the correct and effective use of informatics and communication technologies has led to rapid progress in Communication Technology [24]. Malta Ministry of Information Technologies in 2004 identified 13 strategic goals made and published. This strategy covers the current period as well as branding strategy Intelligent Island in 2008-2010 (The Smart Island strategy), as a result of Malta's strategy was done in previous years occurred.

Government and including the industrial action Informatics of the new generation in this package and Communication Technology infrastructure and development, intelligent workforce development, a better life using information and communications technologies for the quality, improve public services and to facilitate the management is of the e-commerce development objectives [24] [25]. In 2000, only 28% of the Maltese Maltese citizens are using a telephone but in 2007, this rate was 86.6% and in 2013, 137.18% out on the general population of mobile subscriptions **Figure 2**. PCI in 2007 by the NSO and MIIT Malta are given statistics of the Internet and mobile use [14].

Figure 3 gives the statistics of mobile strategy of the Maltese government (Malta Ministry for Investment, Industry and Information Technology, 2008).

Percentage	Indicator	Source
86.6%	Mobile subscriptions as a percentage of population	NSO, 2007
70.3%	Percentage of households with a PC	NSO/MIIIT, 2007
45.9%	Percentage of individuals (18+) using the computer frequency	NSO/MIIIT, 2007
22	Internet subscriptions per 100 persons, not households	NSO, 2007
63%	Individuals with access to the Internet	NSO/MIIT, 2007
80% (of 63%)	Individuals with access to the Internet with a broadband connection	NSO/MIIIT, 2007

Figure 2. PCI in 2007 by the NSO.

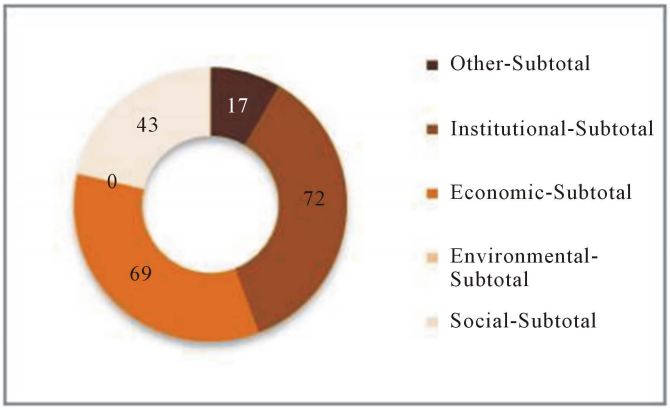


Figure 3. Number of MGOV strategies for SD (Sustainable Development) dimensions—Malta.

According to the statistics of the Maltese government enterprise (72) follow immediately after the economy is mainly a strategy (69) and social development (43) seems to give importance [24]-[27].

Figure 3 shows the strategy of Malta's individual mobile state sustainable development goals. In turn, the development in the Maltese national Information and Communication Technology: corporate through corporate development, services and applications, Innovation Systems and Infrastructure sizes, social development and innovation system, **Figure 4**. The **Figure 5** is an illustration of the tabulated data [28].

Support received from external sources of Malta, the advantage of the small population, it is seen that the source of accurate time and because the site in place using importance is given to the ICT infrastructure and mobile state of development of the state policy today an important place in the mobile state of Malta.

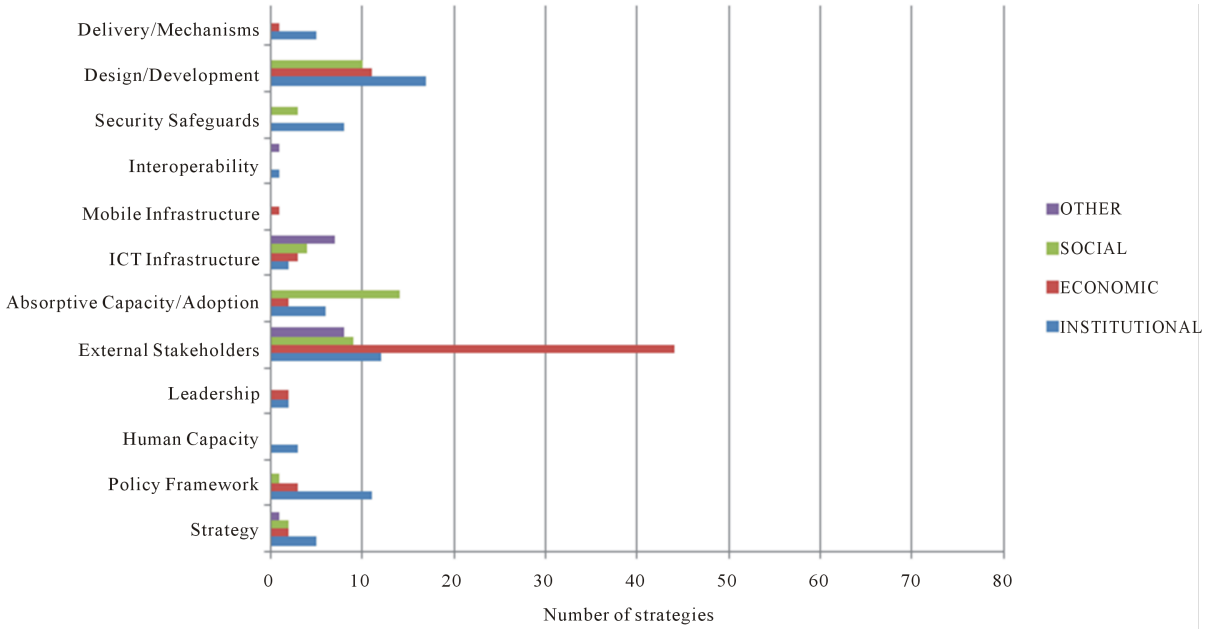


Figure 4. Contribution of MGOV dimensions to SD dimensions—Malta.

SD DIMENSIONS	MGOV DIMENSIONS												
	INSTITUTIONS				INNOVATION SYSTEM		INFRASTRUCTURE				SERVICES APPS		SUM
	Strategy	Policy Framework	Human Capacity	Leadership	External Stakeholders	Absorptive Capacity/ Adoption	ICT Infrastructure	Mobile Infrastructure	Interoperability	Security Safeguards	Design/ Development	Delivery Mechanisms	
INSTITUTIONAL	5	11	3	2	12	6	2	0	1	8	17	5	72
ECONOMIC	2	3	0	2	44	2	3	1	0	0	11	1	69
ENVIRONMENTAL	0	0	0	0	0	0	0	0	0	0	0	0	0
SOCIAL	2	1	0	0	9	14	4	0	0	3	10	0	43
OTHER	1	0	0	0	8	0	7	0	1	0	0	0	17
SUM	10	15	3	4	73	22	16	1	2	11	38	6	201

Figure 5. Detailed contribution of MGOV dimensions to SD dimensions—Malta.

M-Government in Singapore (Institutions & Development & Strategies)

Singapore government's Intelligent Nation 2015 (İn 2015) ICT strategy, m-government strategy has been created in 2005 under the leadership of the Singapore Infocomm Development Agency (IDA) in accordance with the source of their own [29]-[32]. Singapore government in 1980, The National Computerization between 1980-2000 which began as Plan Civil Service Computerization the Programme, to be equivalent to the development of technology and other states has led the strategy of e-government, respectively 2000-2003 e-Government Action Plan 2003-2006 e Government Action Plan 2, 2006-2015 (İn 2015) has planned iGov2010.

E-Government to integrated Government (iGov) strategy aims to; Increasing Reach & Richness of e-Services, Increasing Citizens' Mindshare in e-Engagement, Enhancing Capacity & Synergy in Government, Enhancing National Competitive Advantage. Increasing Reach and richness of e-Services, m-government where the strategy hosting, Infocomm Development Authority of Singapore (IDA) is used by more than 300 mobile applications as active, to be reliable and useful by Singapore citizens has led to its receiving positive feedbacks [33]-[37]. **Figure 5** represents ICT strategies in the Singapore in 2015 [38]-[40].

According to statistics Singapore government provided by most of the development strategies (27), then has allocated respectively ,social and institutional development, (14) and other development goals(11) [41] [42].

Figure 6 shows that Singapore's sustainable development objectives of individual mobile government strategy.

According to priority, Singapore İn 2015 ICT Strategy development: economic development through particular institutions, Innovative systems and infrastructure dimensions, Innovation systems, services and applications with dimensions of social and institutional development, multiple development Another strategy (multiple development) mostly with the aim to advance their goals belongs to the infrastructure and innovation system. The **Figure 8** is a tabular representation of the data shown in **Figure 7** [43].

The MGOV dimensions presents a consolidated pool of MGOV strategies according to the four dimensions of the MGOV framework; Institutions, Innovation System, Infrastructure and Services and Applications [44][45]. The SD Dimensions defined as "Development that meets the needs of the present without compromising the ability of future generations to meet their own needs."

Singapore state e-government and m-government gives rise to slower progress because of Less of the outsourcing of the Singapore government is more than the population, and the recycling (feedback) to be healthy, resource allocation to as the state's need for ICT and infrastructure.

5. Conclusions

In conclusion, this study's findings show that e-government to m-government is inevitable. ICT is no longer a branch of technology sees leverage for all sectors. The small island developing States, Malta and Singapore mobile government between were compared with how efficient and effective use and as a result.

Malta began to mobile government application development in 2002. The small population has become easier to get feedback. We also have a strong external sources of Malta, the large budget allocation to the mobile state in terms of internal resources and Malta can be said referring to the support received from the European Union that, Malta has used although a small island country mobile government applications effectively and efficiently.

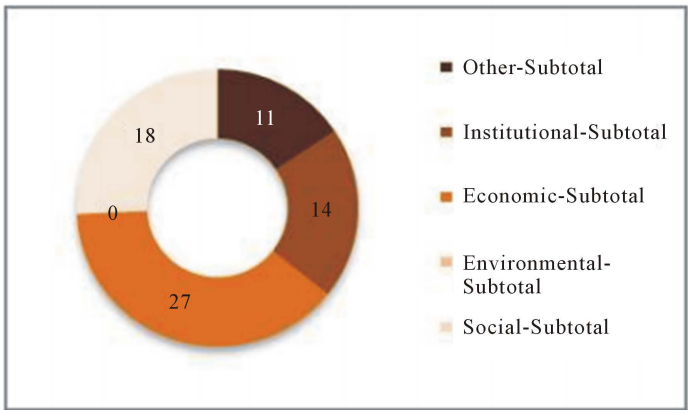


Figure 6. Number of MGOV strategies for SD dimensions-Singapore.

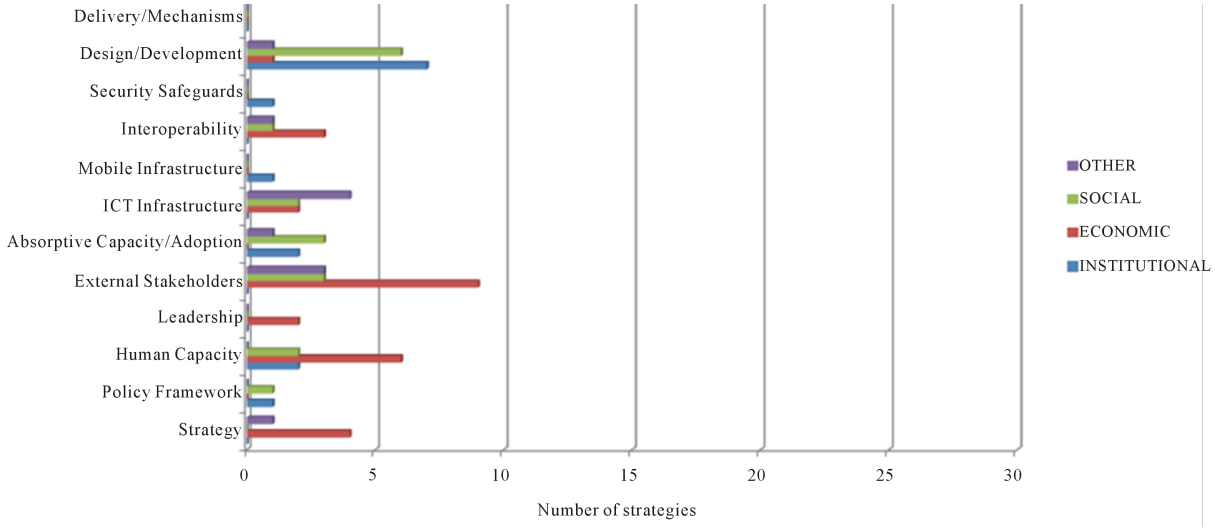


Figure 7. Contribution of MGOV dimensions to SD dimensions—Singapore.

SD DIMENSIONS	MGOV DIMENSIONS												
	INSTITUTIONS				INNOVATION SYSTEM		INFRASTRUCTURE				SERVICES APPS		SUM
	Strategy	Policy Framework	Human Capacity	Leadership	External Stakeholders	Absorptive Capacity/ Adoption	ICT Infrastructure	Mobile Infrastructure	Interoperability	Security Safeguards	Design/ Development	Delivery Mechanisms	
INSTITUTIONAL	0	1	2	0	0	2	0	1	0	1	7	0	14
ECONOMIC	4	0	6	2	9	0	2	0	3	0	1	0	27
ENVIRONMENTAL	0	0	0	0	0	0	0	0	0	0	0	0	0
SOCIAL	0	1	2	0	3	3	2	0	1	0	6	0	18
OTHER	1	0	0	0	3	1	4	0	1	0	1	0	11
SUM	5	2	10	2	15	6	8	1	5	1	15	0	70

Figure 8. Detailed contribution of MGOV dimensions to SD dimensions—Singapore.

The Singapore government has begun in 1980 to develop mobile applications acted under separate plans each year until 2005. But in 2005, it acted according to plan named Infocomm which was the 10-year plan valid until 2015. Singapore's not too much government budget allocation to the mobile application from its internal budget , less external sources, causes of not too much developing in mobile government. In addition to making any conscious attempt to make it difficult to get feedback because of crowded population of the population is among the reasons why more states develop mobile applications.

References

[1] (2014) Base Souce: Mobile Governance for Small Island Developing States—Strategy Knowledge Base.

[2] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[3] Kuschu, İ. and Kuschu, H. (2004) From E-Government to M-Government: Facing the Inevitable. MgovLab.

[4] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94.

http://dx.doi.org/10.5121/ijasuc.2012.3306

[5] Özbilgin, G. and Çalış, K. (2013) General Comparison of Information and Communication Technologies in Turkey and Azerbaijan.

[6] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[7] Kocacık, F. (2003) Information Society and Turkey. University of Cumhuriyet, Social Science Magazine.

[8] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[9] Erkul, E. (2008) M-Government around the World. eTR Awards and Conference.

[10] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education, United Kingdom*, **2**, 1-6.

[11] United Nations E-Government Survey (2014) E-Government for the Future We Want.

[12] Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. *Global Journal of Sociology*, **4**, 41-45.

[13] Türkiye Bilişim Derneği (TBD) KAMU BİLGİ İŞLEM MERKEZLERİ BİRLİĞİ ÇALIŞMA GRUBU (KAMU-BİB)- "Türkiye'de E-devlet Nasıl Olmalı?"

[14] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18. http://dx.doi.org/10.14738/tmlai.25.430

[15] Malta Information Technology Agency (2012) Strategic Plan 2009-2012.

[16] Osterwalder, A. (2015) ICT in Developing Countries.

[17] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[18] Sandy, G.A. and McMillan, S. (2005) A Success Factors Model for M-Government. EURO mGOV 2005, Brighton, 349-358.

[19] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[20] Oswin, N. and Yeoh, B.S.A. (2010) Introduction to the Special Issue: Mobile City Singapore. *Mobilities*, **5**, 167-175.

[21] Sari, A., Karaduman, A. and Firat, A. (2015) Deployment Challenges of Offshore Renewable Energy Systems for Sustainability in Developing Countries. *Journal of Geographic Information System*, **7**, 465-477. http://dx.doi.org/10.4236/jgis.2015.75037

[22] CAPAM 2008 Conference, Barbados "Mobile Government".

[23] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

[24] National Statistics Office (2012) ICT Usage by Enterprises and Households 2011. National Statistics Office, Valletta.

[25] Sari, A. and Mahmutoglu, H. (2013) Potential Issues and Impacts of ICT Applications through Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **89**, 585-592. http://dx.doi.org/10.1016/j.sbspro.2013.08.899

[26] Sari, A. (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. *International Journal of Learning and Development*, **2**, 18-30. http://dx.doi.org/10.5296/ijld.v2i2.1371

[27] The National ICT Strategy for Malta (2008-2010). The Smart Island. http://unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN034350.pdf

[28] Güler, M. and Döventaş, E. (2009) Elektronik Devletten (E-Devlet) Mobil Devlete (M-Devlet) Geçişte Türkiye'de Yerel Yönetim Uygulamalari.

[29] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[30] Trimi, S., Lee, S.M. and Tan, X. (2005) Current Practices of Leading E-Government Countries. *Communications of the*

ACM, **48**, 99-104.

[31] Ghyasi, F. and Kushchu, I. (2004) M-Government: Cases of Developing Countries. mGovLab, International University of Japan, Niigata Prefecture.

[32] Al-Khamayseh, S., Lawrence, E. and Zmijewska, A. (2006) Towards Understanding Success Factors in Interactive Mobile Government. University of Technology, Sydney.

[33] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. *Proceedings of the* 2013 *Fifth International Conference on Computational Intelligence*, *Communication Systems and Networks* (CICSyN), Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/CICSYN.2013.79

[34] Al-khamayseh, S. and Lawrence, E. (2006) Towards Citizen Centric Mobile Government Services: A Roadmap.

[35] Sari, A. (2014) Influence of ICT Applications on Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **116**, 4939-4945. http://dx.doi.org/10.1016/j.sbspro.2014.01.1053

[36] Digital Services Advisory Group and Federal Chief Information Officers Council (2012) Government Use of Mobile Technology.

[37] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. In: *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN'13*), ACM Press, New York, 454-456. http://doi.acm.org/10.1145/2523514.2523586 http://dx.doi.org/10.1145/2523514.2523586

[38] Negroponte, N. (1998) One Room Schools. Wired 09/06/98.

[39] University of Hitit Social Science Institute Magazine, June 2009 (25-48).

[40] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. *Proceedings of the* 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582. http://doi.acm.org/10.1109/TAEECE.2013.6557339.

[41] Mobile Governance for Small Island Developing States—Strategy Knowledge Base, 28 April 2014.

[42] Singapore Infocomm Development Agency, 2006.

[43] The Brundtland Commission (1987) Report of the World Commission on Environment and Development: Our Common Future. Oxford University Press, Oxford.

[44] Oui-Suk, U. (2010) Introduction of m.Government & IT Convergence Technology. Working Document, KAIST Institute for IT Convergence, Daejeon.

[45] The White House (2014) Digital Government, Building a 21st Century Platform to Better Serve the American People. The Executive Office of the President of the United States. http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

Int. J. Communications, Network and System Sciences, 2015, 8, 552-566
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813050

Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)

Arif Sari[1], Onder Onursal[2], Murat Akkaya[1]

[1]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
[2]Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
Email: arifsari@gau.edu.tr, oonursal@eul.edu.tr, muratakkaya@gau.edu.tr

Received 22 April 2015; accepted 27 December 2015; published 30 December 2015

Abstract

There is a significant increase in the rates of vehicle accidents in countries around the world and also the casualties involved ever year. New technologies have been explored relating to the Vehicular Ad Hoc Network (VANET) due to the increase in vehicular traffic/congestions around us. Vehicular communication is very important as technology has evolved. The research of VANET and development of proposed systems and implementation would increase safety among road users and improve the comfort for the corresponding passengers, drivers and also other road users, and a great improvement in the traffic efficiency would be achieved. This research paper investigates the current and existing security issues associated with the VANET and exposes any slack amongst them in order to lighten possible problem domains in this field.

Keywords

Vehicular Ad Hoc Network (VANET), MANET, Vehicle-to-Vehicle (V2V) Communication, Vehicle-to-Infrastructure (V2I) Communication

1. Introduction

The road has become a "moving network", today vehicles are been designed to carry networks, communicate with other vehicles via a communication link or channel. The 2009 Urban Mobility Report, issued by the Texas Transportation Institute, reveals that in 2007, the congestion caused Urban Americans to travel 4.2 billion hours more and to purchase an extra 2.8 million gallons of fuel [1] [2]. This caused a great cost of 187.2 $billion and an increase of 50% and above in the previous decade [1] [2].

Recently, the attention of institutes and industries on VANET has grown vastly due to the promising features. The communication between vehicles has created a research field that can enhance the security and the effi-

How to cite this paper: Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *Int. J. Communications, Network and System Sciences*, **8**, 552-566.
http://dx.doi.org/10.4236/ijcns.2015.813050

ciency of transportation system, traffic conditions and also non-safety measures like weather information, location etc. [3]-[5].

According to configuration of network, VANET can be divided into three categories namely: Wireless Wide Area Network (WWAN), Hybrid Wireless Architecture, and Ad Hoc V2V communication. In the WWAN, the access point of the cellular gateway are fixed, this allows the direct communication between the vehicle and the access point. The Hybrid wireless Architecture uses WWAN access points at some points in the network, while the communication between those access points in the Hybrid Wireless Architecture are achieved with the use of Ad Hoc communications. The third category is the Ad Hoc Vehicle-to-Vehicle communication; this doesn't require any fixed access point for the vehicles to communicate. Vehicles are designed with their own wireless network card and the setting up of an Ad Hoc network can be actualized for each vehicle.

VANET is a subsystem of Mobile Ad Hoc Network (MANET), VANET communicates with the MANET-like technology with the equipment nearby along the road side, and also to communicate between vehicles. Their characteristics are different from that of other networks [3]-[5]. Unavailability of road information can create a possibility of accurately stating the position of the vehicle at that time. The vehicle is the node in VANET and the nodes are limited to a particular type of topology while in motion which is the road topology. The nodes can provide power for data processing and information transmission to sustain the functioning of the node [4]-[6].

Although VANET possess the characteristics of a wireless network, there's a unique character that is associated to the mobility and the unreliable channel condition [6] [7]. Besides the safety application that VANET provides for the road users, there's also the access to multimedia, mobile e-commerce, weather information etc. [6]-[8]. There are some applications that are specifically designed to aid drivers and improve the services of VANET such as: Advance Driver Assistance System (ADASE2), Crash Avoidance Matrices Partnership (CAMP), NOW (Network on Wheels), Fleet Net, etc. these applications were designed and developed with the joint services of different government and some major car manufactures company [8]-[10].

The paper will discuss about the Vehicular Ad Hoc Networks (VANET) in detail in the Section 2 and discussing about main architecture of VANET in the Section 3. The Section 4 discusses about different classifications of VANET applications and Section 5 discusses about main characteristics of VANETs. The common VANET units and entities in classification of environment are discussed in Section 6. The VANET communications patterns are classified and explained in 3 main categories as warning broadcast, group communication and beaconing in Section 7. The routing features of VANETs which are geocast, broadcast, unicast and multicast is discussed in Section 8 in detail. In Section 9, security issues discussed which are based on three main categories such as: availability, authenticity, and confidentiality and research is concluded with Section 10.

2. Vehicular Ad Hoc Network (VANET)

Vehicular Ad Hoc Network (VANET) utilizes cars as a mobile node to create a mobile network [13]. Vehicles act as a mobile node with the corresponding network. The basic aim of VANET is to improve and increase the safety on our roads and road users, comfort of passengers, and also aid the communication between vehicles and roadside equipment. The VANET communication medium is installed on each node (vehicle) [11]. As shown in **Figure 1**, each vehicle has its own communication wireless network card which allows ease of communication flow between vehicles and roadside units.

Figure 2 Shows the different domains that exist in VANET. The Mobile Domain consists of (Vehicle and Mobile Devices) such as PDA, Smart Phones, and Laptop etc. The Generic Domain consists of (Internet Infrastructure and Private Infrastructure) such as nodes and servers. While the Infrastructure Domain consists of (Road Infrastructure or Units and the Central Infrastructure) such as the RSU that communicate with the vehicle along the road, and the management center that communicates with the internet.

The Mobile Domain communicates with the Infrastructure Domain and the Infrastructure Domain communicates with the Generic Domain and data flows between the different domain to provide effective and efficient use of the road by the road users.

Since the communication is provided in 2 different way in VANET, there are some fixed node that act as a roadside unit or equipment which enables the ease of VANET to serve as a gateway to the internet and also in accessing geographical data [12]-[14]. Each node in the VANET doesn't only participate in data transmission and receiving, they also act as a wireless router of the network as different nodes communicate via their own

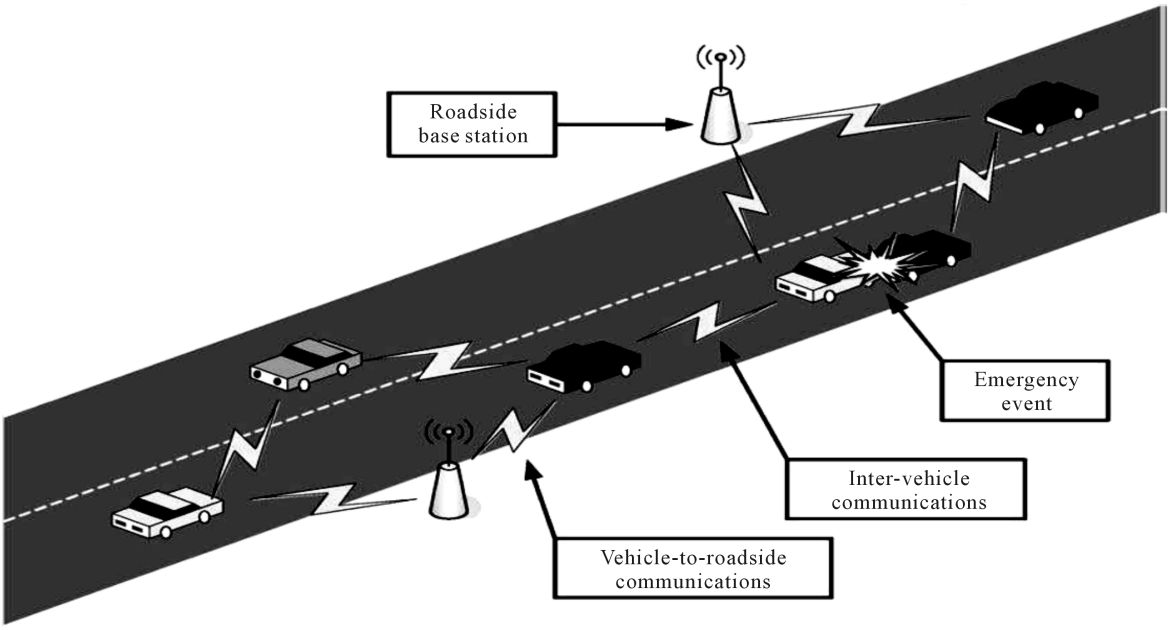


Figure 1. A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give the drivers the time to react to life-endangering events.

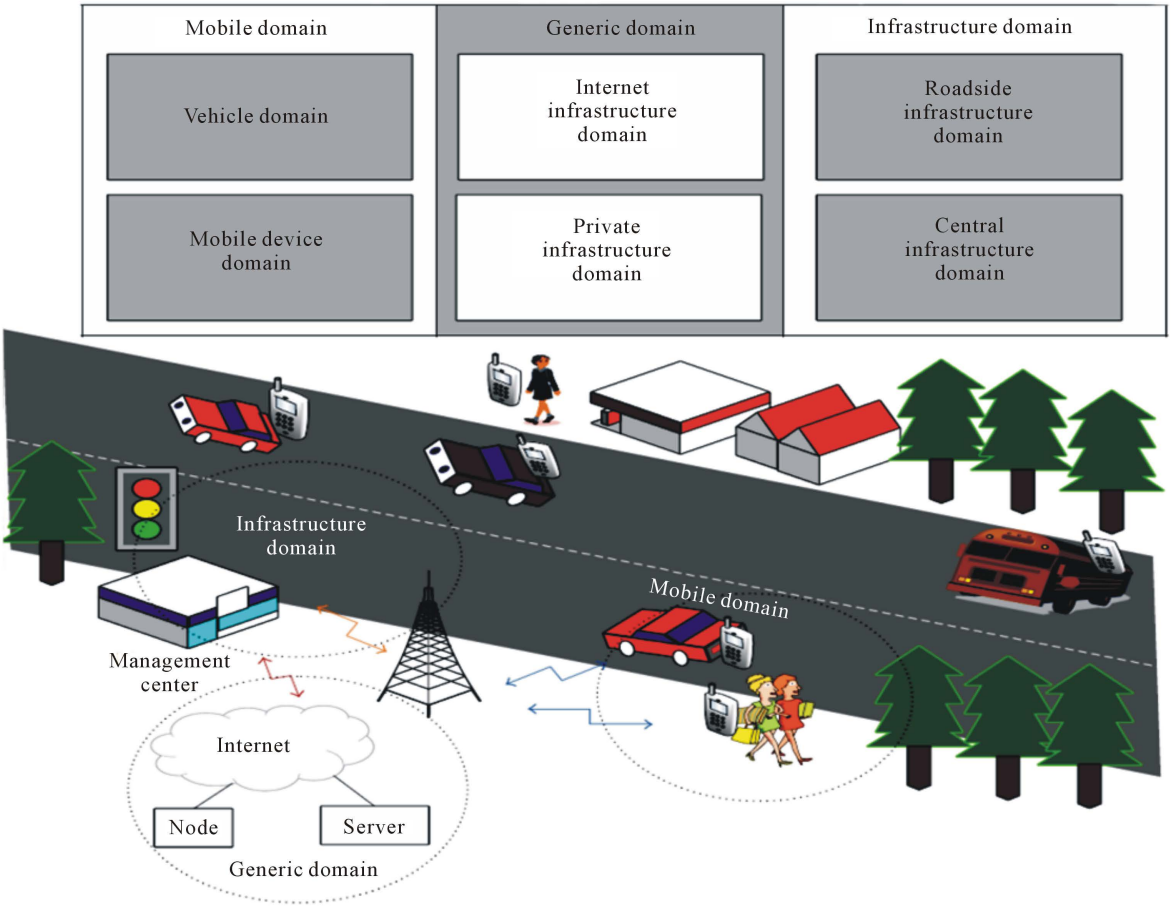


Figure 2. VANET system sphere.

communication range, permitting cars in the region of 100 to 300 meters of each other to join the network, and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created [15].

Components of VANET are onboard units and roadside units as shown in **Figure 3**, we can see how communication is transmitted from the roadside unit to the onboard unit in the vehicle, and also a vehicle to vehicle communication. This creates a better share of information between vehicles.

VANET, vehicles act as nodes, unlike MANET that vehicles are set to move on a predefined road. The vehicles must follow traffic signs and signals and their velocity relies on the speed sign [9]. Wireless devices such as; Personal Digital Assistant (PDA), Remote Keyless Entry Device, Mobile Phones, Laptops etc. are supported by VANET inside the vehicle [16]-[20]. Due to the increase of mobile wireless devices, the demand for the vehicle-to-vehicle (V2V), vehicle-to-roadside (VRC), and vehicle-to-infrastructure (V2I) communication will grow rapidly [20]. There are two type of communication infrastructure available by the VANET; first is the wireless ad hoc network, where there's communication between vehicles without infrastructural support. Secondly, the communication between the vehicle and the road side unit [14]. The IEEE defined standard of establishing a VANET is 802.11 or 802.16 (WIMAX).

Due to the relatively high speed of nodes (vehicles) in the VANET and the clustering of vehicles in a particular location can cause a very large network at that time due to the independency of each node, a communication standard known as the Dedicated Short Range Communication (DSRC) was developed to fix the issue. This communication standard clearly requires the use of Road Side Units (RSUs) that are installed along the road as gateways between the infrastructure and the nodes (vehicles) and also in reverse [21]. The DSRC communicates on a 5.9 GHZ band and uses 802.11 access methods. USA allocated 75 MHZ of spectrum in the 5.9 GHZ, while Europe allocated 30 MHZ of spectrum in the 5.9 GHZ band for DSRC, this is to be utilized by the Intelligent Transportation Systems (ITS) [22].

As shown in **Table 1**, there are 7 MHz wide channels. Four of which are service channels that is used for safety and non-safety applications, and there is a control channel (CCH) which is used to control the channel. The two reserved channel (172 and 178) respectively are for future safety applications. Channel 172 is reserved for high accessibility and low inactivity of applications while channel 178 is reserved for high power public safety applications.

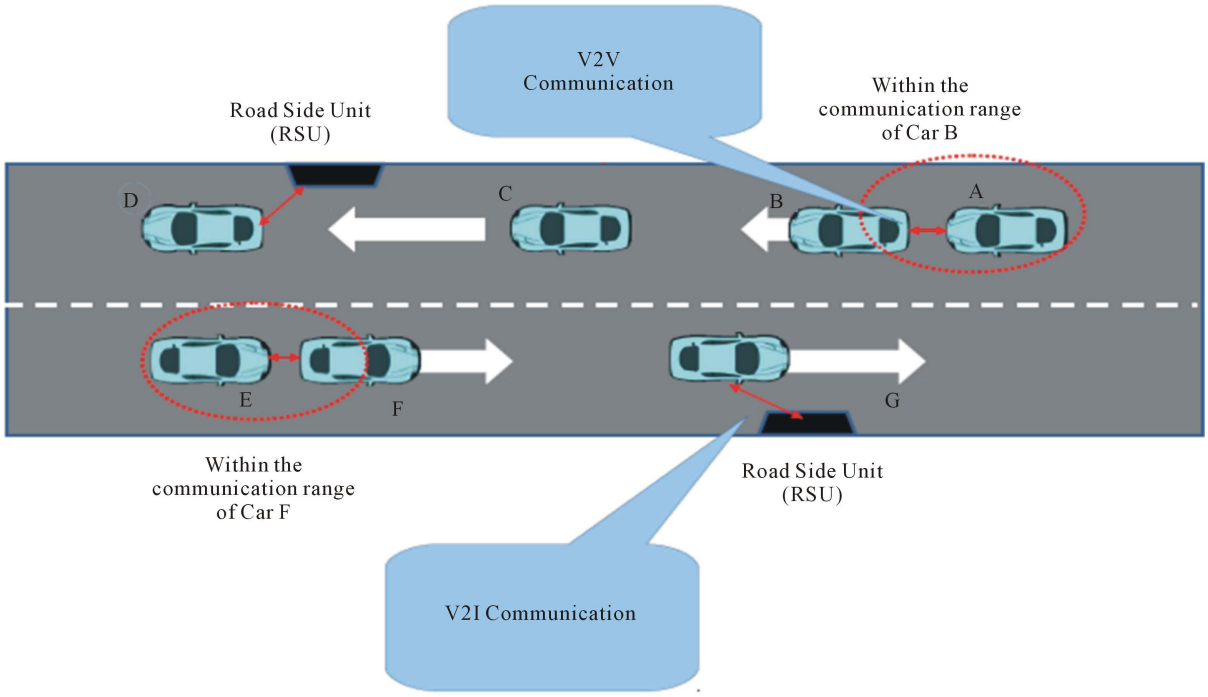


Figure 3. Typical components of VANET.

3. Layered Architecture for VANET

The OSI model group similar communication functions into one of the seven logical layers [23]-[25]. In VANET, the session and the presentation layers are omitted and a particular layer can be further broken or partitioned into sub layers in the VANET architecture, as illustrated in **Table 2** below [25]. The architecture of VANET may change in different regions, and the protocols and interface will also be different. As shown in **Table 3**, the protocol stacks for the Dedicated Short Range Communication (DSRC) in the US [26]. At various layers, different protocols are designed to be used of which some are still under development [26].

The approved amendment to the IEEE 802.11 standard which is IEEE 802.11p standard adds a wireless access in VANET vehicular environment (WAVE). This is focused primarily on the physical layer and MAC sub layer of the protocol stack. The IEEE 1609 standard is a higher protocol standard compared to the IEEE 802.11p. The IEEE 1609 standard functions in the middle layers of the protocol stack and it adaptably supports the safety applications in VANET. While the nonsafety applications are supported through a different set of protocols. The Network, Transport layer services for the nonsafety applications in VANET are supported or provided by IPV6, TCP, and UDP [27]-[29].

Table 1. DSRC spectrum allocation.

Name	MHz Wide Channels Number	Spectrum Allocated (GHz)
Critical Safety of Life (Reserved)	172	5.860 GHz
Service Channel (SCH)	174	5.870 GHz
Service Channel (SCH)	176	5.880 GHz
Control Channel (CCH)	178	5.890 GHz
Service Channel (SCH)	180	5.900 GHz
Service Channel (SCH)	182	5.910 GHz
High-Power Public Safety (Reserved)	184	5.920 GHz

Table 2. The OSI model in VANET.

Application Layer	
Transport Layer	
Network Layer	
Link Layer	LLC Sublayer
	MAC Sublayer
Physical Layer	PLCB Sublayer
	PMD Sublayer

Table 3. The layered architecture for DSRC.

Safety Applications	**Nonsafety Applications**
Transport and Network Layer IEEE 1609.3	Transport Layer TCP/UDP
Security IEEE 1609.2	Network Layer IPV6
LLC Sublayer IEEE 802.2	
MAC Sublayer IEEE 1609.4	
MAC Sublayer	IEEE 802.11 p
Physical Layer	

4. VANET Applications

There are two categories of applications that is associated with the VANET; safety and user based applications [30].

4.1. Safety Related Applications

The safety related applications are used to increase safety on the road and also that of the road users, such applications are: collision avoidance, cooperative driving, and traffic optimization.

Collision Avoidance: Some studies states that 60% of road accidents can be avoided if the drivers are warned 0.30 seconds before the collision occurs [31]-[33]. In the collision avoidance application, a signal or a nodes location is broadcasted to other nodes if an accident occurs so as to prevent other vehicles coming to get involved.

Cooperative Driving: An uninterrupted/safe journey can be achieved via traffic related warning signals such as changing of lane, the speed limit, negotiating a bend or curve etc. drivers are practically responsible and involved in this application, because many accidents occurs because of the lack of cooperation between drivers [34] [35].

Traffic Optimization: Vehicles acts as data collectors for the VANET. A signal like (JAM, ACCIDENT) etc. can be sent among the vehicles when there's a disruption on the road involving a vehicle or more so they can choose an alternative route to optimize the traffic and save time. For example, if there's a congestion on one lane the information can be transmitted or relayed to the vehicle on the opposite lane so it can be delivered faster to vehicles heading towards the congestion location. This gives enough time to for the vehicles approaching to choose an alternate route [36].

4.2. User Based Applications

Safety comes first in the usage of the road, afterwards other services can be included. Infotainment (Information and Entertainment) services is also provided by VANET, such as:

Peer-to-Peer Application: these application can be utilized usefully to provide music, video, etc. sharing among the vehicles in the network.

Internet Connectivity: VANET provides the road users with internet connectivity

Other Services: Geographical locations, payment services, etc. are provided by non-safety applications in VANET.

5. Characteristics of VANET

As earlier stated VANET is a sub of MANET, but it has its own distinguished characters such as:

High Mobility: Because vehicles move at high speed it is difficult to predict a node position and also it makes protection of nodes privacy hard.

Rapid Changing Network Topology: Due to the random speed of a node (vehicle), node position is difficult to ascertain and its position changes frequently, this causes the network topology to change frequently in VANET.

Unbounded Network Size: VANET network size is not limited to a particular region or locality, it can be implemented for a city or more, or even for countries. VANET is geographically limitless.

Frequent Exchange of Information: Information can be exchanged amongst vehicles and road side units (RSUs) die to the AD Hoc nature of VANET. This makes the information exchange more frequent and updated.

Wireless Communication: The technology that VANET runs on is a wireless technology, therefore nodes are connected and information exchange are done via a wireless communication channel.

Time Critical: Time limits are set on each information packet that is been sent or received, this enables the delivery of information at the right time to avoid unwanted delays and decisions can be made accordingly by the corresponding node with action taken.

Sufficient Energy: The nodes have huge power source, because the vehicles run on their own battery. There's no limited power supply for the corresponding components to function properly. This cause demanding techniques to be used by VANET, such as RSA, ECDSA etc.

Better Physical Protection: Because VANET nodes are vehicles, it's more secured physically. This makes VANET nodes to be more difficult to compromise physically and also reduce physical attack on the infrastructure.

6. VANET Model

In VANET there are different units involved in the deployment. Although majority are nodes (Vehicles), there are other units or entities that keep the basic operations functioning in the network. Due to the large and complex system model, it has been categorized into four sub models namely: Driver and Vehicle Model, Traffic Flow Model, Communication Model, and application Model [37]-[39].

Driver and Vehicle Model: This shows the behavior of a single vehicle. In this model two factors are considered such as: different driving styles and the vehicle characteristics. Example a violent driver or passenger and a sport car [39].

Traffic Flow Model: This model depicts the interaction between vehicles, drivers, and the infrastructure to develop a good road network [39] [40].

Communication Model: This shows the flow of data or information between or among the road users [41].

Application Model: This points out the usefulness in the behavior and quality of cooperative VANET applications [41].

Figure 4 illustrated the VANET units and entities that makes up the VANET model, and it is explained in detail section below.

6.1. Common VANET Units and Entities

There are two different environments generally researched in VANET namely; Infrastructure and Ad-Hoc environment.

6.1.1. Infrastructure Environment

In this environment, units or entities can be interconnected permanently. Inside this environment mainly contains the entities that mange traffic and also gives access to external services. Manufactures are known to be inside this environment of the VANET model; because during manufacturing they identify each vehicle uniquely. Legal authority is also in this environment of VANET model; putting aside the different regulations that binds countries, vehicles registration and offence reporting is ensured. The Trusted Third Party (TTP) are also in this environment [42]. They offer various services such as time stamping and credential management. Manufactures and the Authority are related to (TTP) because the services are needed, example; issuing of electronic credentials [42]. Service providers are also in this environment, because they give out services that can be accessed via the VANET, such services are' Location Based Services (LBS) or Digital Video Broadcasting (DVB) etc. [42].

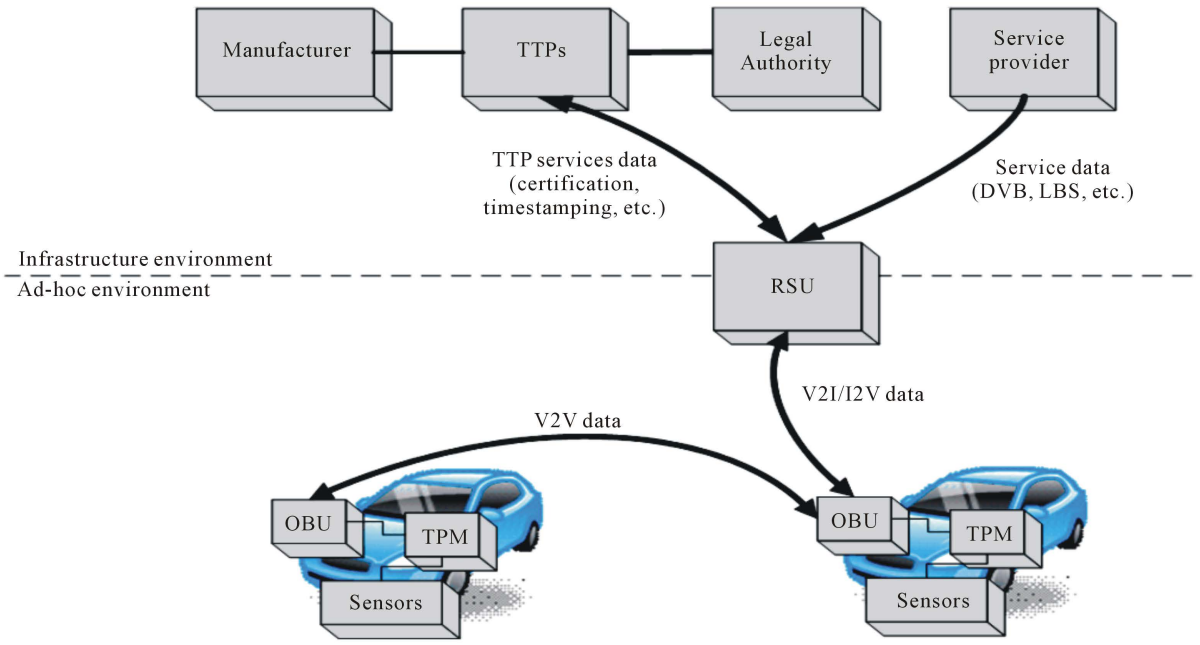


Figure 4. VANET units and entities.

6.1.2. Ad-Hoc Environment

This environment creates ad-hoc communications from vehicles. The vehicles are equipped with 3 different devices namely; On-Board Unit (OBU) that enables the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [23]. The Ad-Hoc environment also have a set of sensors to their status and its environment e.g. (Fuel Consumption, Slippery Road, and Safety Distance). The data gotten can be shared among other node to improve and increase road safety.

A Trusted Platform (TPF) is always installed on the vehicles, such devices are for security purposed and also for computation and reliable storage [43].

7. VANET Communication Patterns

The use of VANET enables the use of several applications from safety to non-safety applications. These applications exchange messages over VANETs and they are used for different proposes. In the VANET they are four different communication pattern identified [44] [45]. Although other communication pattern exists such as (multimedia access, location based services, etc.).

7.1. Vehicle-to-Vehicle (V2V) Warning Broadcast

This communication pattern is useful in a unicast or multicast situation, where message is been sent to a specific or a group of vehicles. For example and emergency vehicle is approaching, a message can be sent to vehicles coming; this will create an easy passage for the emergency vehicle, or when an accident is detected, a message can be sent to arriving vehicles to warn them and also increase safety on the road [46]. This is shown in **Figure 5** below.

7.2. Vehicle-to-Vehicle (V2V) Group Communication

In this communication pattern, only vehicles that share similar features can participate in the communication. Such features can be static or dynamic in nature, that is vehicles of the same manufacture or enterprise (static nature) or vehicles that appears to be in the same area in a particular time interval (dynamic nature) [47] [48]. This is shown in **Figure 6** below.

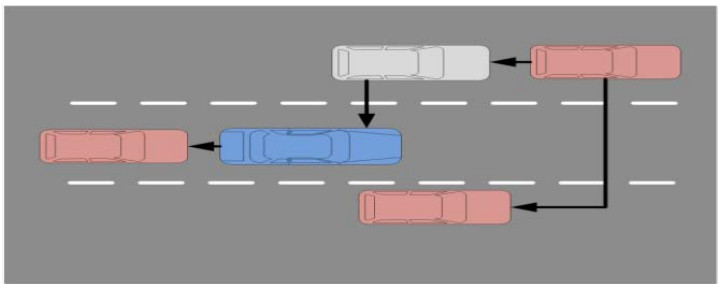


Figure 5. V2V warning broadcast.

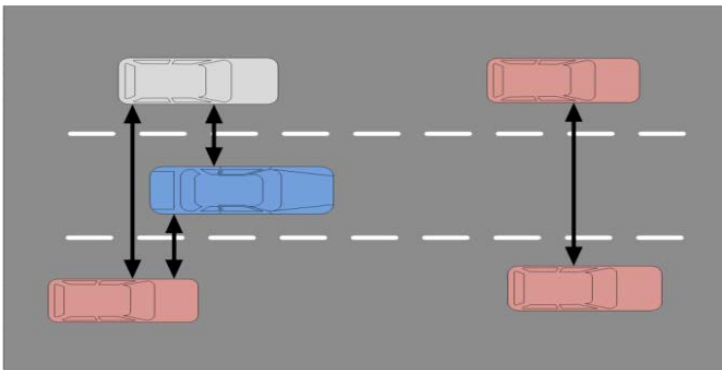


Figure 6. V2V group communication.

7.3. Vehicle-to-Vehicle (V2V) Beaconing

Under this pattern, messages are sent periodically to vehicles that are nearby. These messages contain breaking use, heading, current speed, bend negotiation etc. of the sender or transmitting vehicle. As shown in **Figure 7**, the V2V beaconing communication messages are only sent to 1-hop communication vehicle that is the messages are not forwarded after receiving. This is helpful because the message enables vehicles to discover and access the best neighbor to route a message through or to [49]-[51].

7.4. Infrastructure-to-Vehicle/Vehicle-to-Infrastructure Warning

Messages are relayed either from the infrastructure Road Side Units (RSUs), or from a vehicle to RSUs when a vehicle or RSU spots a potential danger. For example a warning message can be sent from or by the RSU to approaching vehicles heading towards an intersection that a possible collision could happen. This communication pattern is very useful for enhancing road safety [52] [53]. **Figure 8** shows how a warning message was communicated to various nodes to avoid collision.

8. Routing in VANET

In the past few years, routing in VANET have been researched widely [42] [52]-[54]. However, due to the characteristics of VANET having a high active topology recurrent connectivity, the commonly used routing protocols that were implemented for MANET have been tested and evaluated for use in VANET environment [55]. Depending on the number of sending and receiving nodes involved, the routing in VANET can be classified into three types namely; Geocast/Broadcast, Multicast, and Unicast approaches.

8.1. Geocast/Broadcast

This protocol is very important in VANETs. In [56], the review of various geocast/broadcast protocols on VANET was researched on, such as:

- Spatially Aware Packet Routing Algorithm (this protocol is able to predict holes in topology and conduct the geographical forwarding).
- SHDV (this protocol helps find the best path to forward a packet through).

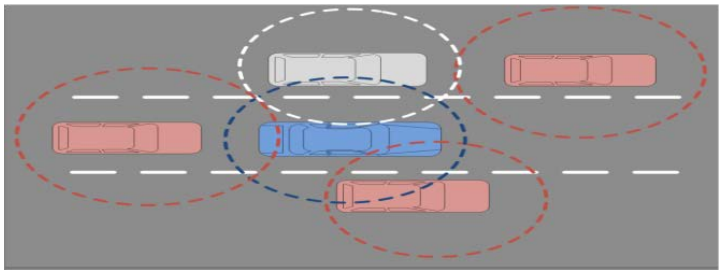


Figure 7. V2V beaconing.

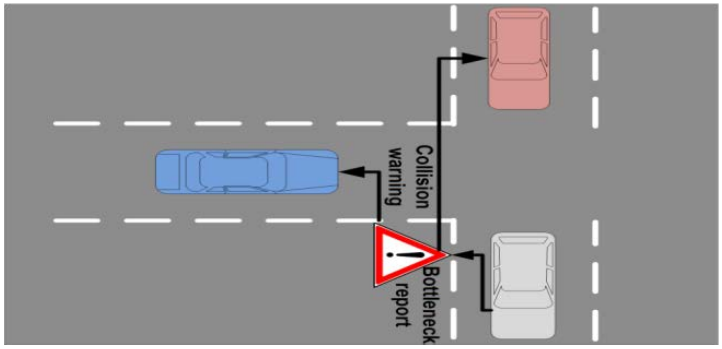


Figure 8. I2V/V2I warning.

- Interface Awake Routing Scheme (this enables the node with a multichannel radio interface and switches the channel based on the SIR evaluation).
- FROV (this selects the retransmission and spans further node to rebroadcast a message).
- Multi-hop Broadcast Protocol (this protocol segments the road and choose the vehicle that is far in a non-empty segment).

Other protocols such as; V-TERADE, UMB, AMB, MHVB, and MDDV have been proposed by other researchers [56].

8.2. Multicast Protocol

Multicast is important among communication between group of vehicles in some vehicular situations such as; road blocks, high traffic density or congestion, accidents, road intersections, bad road surface condition etc. In [56], the multicast protocol was divided into two types, 1) topology based approaches such as ODMRP (this generates a source based multicast mesh and forwards it based on the group address), MAODV (this generates a group based multicast tree), and GHM (this generates group-based multicast meshes). 2) location-based approaches, such as PBM (which is based on positions of all 1-hop neighbors and also that of individual destinations), SPBM (this introduces hierarchal group membership management), LMB (this uses the multicast region as destination information for multicast packets), and RBM and IVG (which define a multicast scope for safety warning messages).

8.3. Unicast Protocol

The unicast communication protocol for VANET is in three ways (as shown in **Table 4**):

- Greedy: in this protocol, nodes forward packets to the vehicle or nodes that are far off neighbor coming towards their destination, like (GYTAR).
- Opportunistic nodes use “carry-toward” technique, where this is done in order to resourcefully deliver the data to the corresponding destination, just like the topology-assist, geo-opportunistic routing etc.
- Trajectory Based: Nodes compute the paths that will possibly lead to the destination and deliver the data by relaying it to nodes that are along one of the computed paths, just like the trajectory-based data forwarding (TBD) [55] [56].

9. VANET Security Issues

Security is always a challenge for any infrastructure that is been used in communication. Safety in VANET is of high priority because human lives are involved. The security challenges or issues must be put in place during the design of VANET architecture [53]-[55]. In [56], the author classified attackers into three categories or dimensions; insider versus outsider, malicious versus rational, and active versus passive.

In VANET security issues, the threats are based into three main groups such as; availability, authenticity, and confidentiality. The following 3 subsections expose these issues in details.

9.1. Threats to Availability

The threats to availability of vehicle-to-vehicle and vehicle-to-roadside communication are:

1) Denial of Service Attack: this kind of attack can be done or carried out by an insider, and or outsiders in the network, such attack causes the network to be unavailable to the authentic users. Flooding and jamming with a high volume generated artificial messages causes the VANET components such as the nodes onboard units and roadside units not to sufficiently process the overload caused by the DoS attack.

2) Broadcast Tampering: This attack is carried out by an insider. It inputs false safety messages into the VANET to inflict damage or harm to the road users. An accident can occur when attacker manipulates the traffic on a specific route.

3) Malware: Virus or works can cause serious interference of flow of operation if introduced into VANET. This attack is often carried out by insiders more than outsiders and also it can be downloaded into the network when a firmware update is done.

4) Spamming: Spam messages in VANET can lead to increased transmission inactivity. This is more difficult to control because there’s no centralized administration.

Table 4. Unicast protocols and algorithms in VANET.

	Protocols/Algorithms	Main Ideas
GREEDY	Geographical source routing (GSR)	Determines the destination location by RLS (reactive location service)
	Greedy perimeter geographic routing (GPCR)	The packet is greedily forwarded to the junction node (coordinator)
	Improved greedy traffic-aware routing (GyTAR)	Selects junctions based on vehicles traffic density and distance to the destination
	Connectivity-aware routing (CAR)	1) Greedy forwarding between anchor points along the selected path 2)The packet is forwarded to a node closer to an anchor point
OPPORTUNISTIC	OPERA: Opportunistic Packet Relaying in disconnected vehicular ad hoc networks	1) Vehicles moving in the same direction are grouped into clusters 2) Opportunistic technique is used to select a better available path
	Topology-assist geo-opportunistic routing	Uses two-hop beacons for the selection of a forwarding node
	MaxProp	1) Uses packet priorities to maximize delivery 2) Includes three stages: neighbor discovery, data transfer, and storage management
	SiFT	A data forwarder selection decision is shifted from the sender to receiver
TRAJECTORY	Geographical opportunistic routing (GeOpps)	A data forwarder is selected based on the trajectory information of individual vehicles
	Trajectory-based data forwarding (TBD)	Is based on vehicle trajectory information and traffic statistics
	Two-level trajectory-based routing (TTBR)	1) The communication area is divided into cells of a grid 2) A grid based location system is applied where some peer servers are distributed

5) Black Hole Attack: This form of attack is cause by nodes refusing to participate in the network or when a node drops out of the network, when this happens all communication routes and link it had before would be broken, this causes a failure in broadcasting message.

9.2. Threats to Authenticity

In VANET authenticity provision is very important. This includes the protecting of legitimate node from the attackers "insider or outsider" infiltrating the network with fake identifies, such threats are:

1) Masquerading: This attack is different from others and it's easier to carry out. The attacker joins the network by having to get a functioning onboard unit and the attacker possess as a legitimate vehicle in the network, variety of attack can be carried out or feasible such as creating of false message and forming of black holes.

2) Global Positioning System (GPS) Spoofing: Global positioning system keeps a location table that holds the geographical locations of all vehicles on the network and their identities. An attack can be carried out using the GPS spoofing through GPS satellite simulator to create a false location on the GPS system in the network, thereby causing the vehicle to think that the corresponding location is the right one. This is because the GPS satellite simulator can generate signals that are way stronger than that generated by the authentic or real satellite.

3) Replay Attack: In this attack, the attacker reinsert packets that have been previously used by nodes into the network, this can poison a node's location table by replaying bacons. Although VANET that operate in the WAVE framework are protected from this attack, but to continue protection a precise source of time should be kept and organized because it is used to keep cache of recently received messages in contrast of the incoming messages.

4) Tunneling: An attacker utilizes the momentarily loss of a vehicle positioning system when it goes through a tunnel before resurfacing on the other side to receive its positioning information. The attacker quickly injects

false positioning information or data in to the onboard unit of the node, causing the node to assume that the information received is valid.

5) Position Faking: In VANET, vehicles are responsible for the detailing of their own position or location information. This makes impersonation nearly impossible. Unsecured communication link or channel can create a blind spot where attackers can quickly modify or falsify their own position or that of other vehicles, create additional identities also known as (Sybil Attack), or even block vehicles from receiving and relaying vital and authentic safety messages.

6) Message Tampering: In this attack, the attacker alters or modify the message that's been relayed or exchanged from vehicle-to-vehicle or vehicle-to-roadside unit communication in order to forge application request or response from other nodes.

7) Message Suppression/Fabrication/Alteration: The attacker physically disables the communication link between vehicles or modifies the application so that the vehicle cannot send or receive or respond to application beacons.

8) Sybil Attacks: In VANET, periodic messages are 1-hop broadcast, this is for securing the physical layer. When the network is not secured an attacker can partition the network and make delivery safety message impossible.

9.3. Threats to Confidentiality

Messages that are exchanged between nodes (vehicles) in VANET are open to confidentiality threats or attack with techniques such as illegitimate collection of messages through eavesdropping and passive attacks which are stated in the literature by the researchers.

10. Conclusions

VANET is an area of research that holds promising future and for vehicular users. However, it has its own challenges in the security prospect. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The unique nature of VANET springs up issues like illegal tracking and jamming of the network. In this paper, we introduced VANET, its architecture, components, communication pattern and issues in its security. In the course of this research, we found out the routing protocols used in VANET that enabled road users to communicate and receive messages appropriately, such as: Geocast/ Broadcast, Multicast, and Unicast protocol. Also VANET communication pattern, entities and characteristics which include: High Mobility, Rapid Changing, Network Topology, Unbounded Network Size, Frequent Exchange of Information, Wireless Communication, Time Critical, Sufficient Energy and better Physical Protection. The characteristics of VANET expose the usability and efficiency in VANET.

With more research done on the security issues of VANET, I believe that VANET will cause a technological change and improvement for the road users. Useful information exchange can prevent future damage and accidents on our road. Future research would be conducted on comparing the various data security mechanisms and their performance metrics.

References

[1] Kadum, A. (2013) A Survey on Vehicular Ad Hoc and Sensor Networks (VASNET).

[2] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306

[3] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[4] Sivasakthi, M. and Suresh, S. (2013) Research on Vehicular Ad Hoc Networks (VANETs): An Overview. *Journal of Applied Sciences and Engineering Research*, **2**, 23-27.

[5] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education, United Kingdom*, **2**, 1-6.

[6] (2011) Vehicular Ad Hoc and Sensor Networks—Principles and Challenges. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing* (*IJASUC*), **2**.

[7] Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE Vehicular Technology Magazine*, **2**, 12-22.

[8] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[9] Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE of Vehicular Technology Magazine*, **2**, 12-22. http://dx.doi.org/10.1109/MVT.2007.912927

[10] Saha, A.K. and Johnson, D.B. (2004) Modelling Mobility for Vehicular Ad Hoc Networks. *ACM International Workshop on Vehicular Ad Hoc Networks*, Philedelphia, 91-92.

[11] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[12] Manvi, S.S., Kakkasageri, M.S. and Mahapurush, C.V. (2009) Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols in Vehicular Ad Hoc Network Environment. *International Conference on Future Computer and Communication*, Kuala Lumpar, 3-5 April 2009, 21-25.

[13] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN* '13). Aksaray, 26-28 November 2013, 454-456. http://dx.doi.org/10.1145/2523514.2523586

[14] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 5*th International Conference on Computational Intelligence, Communication Systems and Networks* (*CICSyN*), Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[15] Bernsen, J. and Manivannan, D. (2008) Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service. *The* 4*th International Conference on Wireless and Mobile Communications*, Athens, 27 July-1 August 2008, 1-6. http://dx.doi.org/10.1109/icwmc.2008.15

[16] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. and Nemoto, Y. (2007) A Stable Routing Protocol to Support ITS Services in VANET Networks. *IEEE Transactions on Vehicular Technology*, **56**, 3337-3347. http://dx.doi.org/10.1109/TVT.2007.906873

[17] Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. *Global Journal of Sociology*, **4**, 41-45.

[18] Hartenstein, H. and Laberteaux, K.P. (2008) A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communication Magazine*, **46**, 164-171.

[19] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[20] Eichler, S., Ostermaier, B., Schroth, C. and Kosch, T. (2005) Simulation of Car-to-Car Messaging: Analyzing the Impact on Road Traffic. *IEEE ASCOTS*, 507-510.

[21] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

[22] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[23] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[24] Gerlach, M. (2006) Full Paper: Assessing and Improving Privacy in VANETs. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=84FC4EF0852B23FBF15CF35E16E0450D?doi=10.1.1.84.8167&rep=rep1&type=pdf

[25] Dahiya, A. and Chauhan, R. (2010) A Comparative Study of MANET and VANET Environment. *Journal of Computing*, **2**.

[26] Sesay, S., Yang, Z. and He, J.H. (2004) A Survey on Mobile Ad Hoc Network. *Information Technology Journal*, **3**, 168-175. http://dx.doi.org/10.3923/itj.2004.168.175

[27] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582. http://dx.doi.org/10.1109/TAEECE.2013.6557339

[28] Toor, Y., Muhlethaler, P. and Laouiti, A. (2008) Vehicle Ad Hoc Networks: Applications and Related Technical Issues. *IEEE Communications Surveys & Tutorials*, **10**, 74-88. http://dx.doi.org/10.1109/comst.2008.4625806

[29] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18. http://dx.doi.org/10.14738/tmlai.25.430

[30] Hu, Y.-C. and Laberteaux, K. (2006) Strong Security on a Budget. Wksp. Embedded Security for Cars. http://www.laberteaux.org/papers/vanet08-epidemic.pdf

[31] Raya, M. and Hubaux, J. (2005) The Security of Vehicular Ad Hoc Networks. *Proceedings of the* 3*rd ACM Workshop on Security of Ad Hoc and Sensor Networks* (*SASN* 2005), Alexandria, 7-10 November 2005, 11-21. http://dx.doi.org/10.1145/1102219.1102223

[32] Robinson, C.L., Caminiti, L., Caveney, D. and Laberteaux, K. (2006) Efficient Coordination and Transmission of Data for Cooperative Vehicular Safety Applications. *In VANET*'06: *Proceedings of the* 3*rd International Workshop on Vehicular Ad Hoc Networks*, New York, 10-19.

[33] Sari, A. and Mahmutoglu, H. (2013) Potential Issues and Impacts of ICT Applications through Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **89**, 585-592. http://dx.doi.org/10.1016/j.sbspro.2013.08.899

[34] Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., *et al*. (2006) Attacks on Inter-Vehicle Communication Systems—An Analysis. *International Workshop on Intelligent Transportation*, Hamburg, 189-194.

[35] Buttyan, L. and Hubaux, J.-P. (2001) Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Swiss Federal Institute of Technology, Laussane.

[36] Sari, A. (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. *International Journal of Learning and Development*, **2**, 18-30. http://dx.doi.org/10.5296/ijld.v2i2.1371

[37] Callandriello, G., Papadimitratos, P., Lloy, A. and Hubaux, J.-P. (2007) Efficient and Robust Pseudonymous Authentication in VANET. *International Workshop on Vehicular Ad Hoc Networks*, Montreal, 9-14 September 2007, 19-28.

[38] Boneh, D. and Shacham, H. (2004) Group Signatures with Verifier-Local Revocation. *Proceedings of the* 11*th ACM Conference on Computer and Communications Security*, Washington DC, 25-29 October 2004, 168-177. http://dx.doi.org/10.1145/1030083.1030106

[39] Armstrong Consulting Inc. (n.d.). Dedicated Short Range Communications (DSRC) Home. Retrieved October 2009. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[40] Sakib, R.K. and Reza, B. (2010) Security Issues in VANET.

[41] de Fuentes, J.M., González-Tablas, A.I. and Ribagorda, A. (2010) Overview of Security Issues in Vehicular Ad-Hoc Networks.

[42] Harsch, C., Festag, A. and Papadimitratos, P. (2007) Secure Position-Based Routing for VANETs. *Proceedings of IEEE* 66*th Vehicular Technology Conference*, *VTC*-2007, Baltimore, 30 September-3 October 2007, 26-30. http://dx.doi.org/10.1109/vetecf.2007.22

[43] Sari, A. (2014) Influence of ICT Applications on Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **116**, 4939-4945. http://dx.doi.org/10.1016/j.sbspro.2014.01.1053

[44] Sun, S., Kim, J., Jung, Y. and Kim, K. (2009) Zone-Based Greedyperimeter Stateless Routing for VANET. *Proceedings of International Conference on Information Networking*, *ICOIN* 2009, Chiang Mai, 21-21 January 2009, 1-3.

[45] Yu, D. and Ko, Y.-B. (2009) FFRDV: Fastest-Ferry Routing in DTN-Enabled Vehicular Ad Hoc Networks. *Proceedings of* 11*th International Conference on Advanced Communication Technology*, **2**, 1410-1414.

[46] Ali, S. and Bilal, S. (2009) An Intelligent Routing Protocol for VANETs in City Environments. *Proceedings of* 2*nd International Conference on Computer, Control and Communication*, *IC*4 2009, Karachi, 17-18 February 2009, 1-5. http://dx.doi.org/10.1109/ic4.2009.4909249

[47] Yang, J. and Fei, Z. (2013) Broadcasting with Prediction and Selective Forwarding in Vehicular Networks. *International Journal of Distributed Sensor Networks*, **2013**, Article ID: 309041. http://dx.doi.org/10.1155/2013/309041

[48] Chen, W., Guha, R.K., Taek, J.K., Lee, J. and Hsu, I.Y. (2008) A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad-Hoc Networks. *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety* (*ICVES* '08), Columbus, 22-24 September 2008, 328-333.

[49] Wahid, A., Yoo, H. and Kim, D. (2010) Unicast Geographic Routing Protocols for Inter-Vehicle Communications: A Survey. *Proceedings of the* 5*th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wire Networks* (*PM2HW2N* '10), Bodrum, 17-21 October 2010, 17-24. http://dx.doi.org/10.1145/1868612.1868616

[50] Moustafa, H. and Zhang, Y. (2009) Vehicular Networks: Techniques, Standards, and Applications. CRC Press, Boca Raton. http://dx.doi.org/10.1201/9781420085723

[51] https://www.academia.edu/8721918/VANET_Vehicle_Ad_hoc_Networks

[52] http://en.wikipedia.org/wiki/OSImodel

[53] Hartenstein, H. and Laberteaux, K. (2010) VANET-Vehicular Applications and Inter-Networking Technologies. John Wiley & Sons, Hoboken.

[54] Maier, M.W., Emery, D. and Hilliard, R. (2004) ANSI/IEEE 1471 and Systems Engineering. *Systems Engineering*, **7**, 257-270. http://dx.doi.org/10.1002/sys.20008

[55] https://en.wikipedia.org/wiki/IEEE_802.11p

[56] Kosch, T., Schroth, C., Strassberger, M. and Bechler, M. (2012) Automotive Internetworking. Wiley, New York. http://dx.doi.org/10.1002/9781119944737

Int. J. Communications, Network and System Sciences, 2015, 8, 567-577
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813051

Scientific Research Publishing

Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks

Arif Sari, Mehmet Karay

Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: arifsari@gau.edu.tr, mehmetkaray@gau.edu.tr

Received 20 August 2015; accepted 10 September 2015; published 30 December 2015

Abstract

There have been various security measures that deal with data security in wired or wireless network, where these measures help to make sure that data from one point to another is intact, by identifying, authenticating, authorizing the right users and also encrypting the data over the network. Data communication between computers has brought about countless benefits to users, but the same information technologies have created a gap, a vulnerable space in the communication medium, where the data that's been exchanged or transferred, thereby causing threats to the data. Especially data on wireless networks are much exposed to threats since the network has been broadcasted unlike a wired network. Data security in the past dealth with integrity, confidentiality and ensuring authorized usage of the data and the system. Less or no focus was placed on the reactive approach or measures to data security which is capable of responding properly to mitigate an attacker and avoid harm and also to prevent future attacks. This research is going to expose the mechanisms and measures of data security in wireless networks from the reactive security approaches point of view and exposes the reactive approaches used to enhance data security.

Keywords

Reactive Security, Data Security, Mobile-Wireless Network, Proactive Security, Encryption, Decryption, Cryptography

1. Introduction

Securing data have not been completely achieved over the years due to different network types and their characteristics, but to a more percentage, data have been secured over a secure network as well. The flexibility of

How to cite this paper: Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *Int. J. Communications, Network and System Sciences*, **8**, 567-577.
http://dx.doi.org/10.4236/ijcns.2015.813051

wireless network always makes the access to the network open, because the SSID is always broadcasting. Data are transferred through the use of radio waves and thus making the data available through everywhere in space, enabling the corresponding users to receive the information anytime with the right device in this case a radio receiver. Due to this data protection becomes a pressing issue to deal with. Wired networks are traditionally protected or secured via firewalls, shields etc. while this cannot be done in the case of wireless data protection. Protecting data in wireless environment or networks need a different mechanism altogether, in order to give the users a secure feel in data transfer and have accuracy, reliability, availability, integrity, and confidentiality.

In a world of diverse communication between nodes, wired and wireless devices, and mobile-wireless devices. Data communication has reached a significant point in Information Technology that security of data gives the user an opportunity to share or exchange information securely using the right and appropriate tool. Today banks, government, defense systems all have changed the way data are been exchanged or transmitted, transactions have been compromised in different ways. The communication medium that is been used for data communication are vulnerable to different attacks. The protection of these systems is very important and prominent and this leads to more attacks and loss of important and confidential information when the right measure or system is not installed [1] [2]. Threats come from hackers, spies, corporate raiders, terrorists, professional criminals etc. Their objective is either financial or political gain [1] [2]. In trying to solve the security challenge of today's threats, network professionals became aware of the Proactive and Reactive approach to tackling security vulnerabilities [1] [2]. The Proactive approach secures data by predicting the future of an attack and tends to mitigate that attack. While the reactive approach on the other hand learns from the past attack and use that knowledge to prevent future attacks from happening [1] [2]. The reactive approach to data security in mobile-wireless network is like an Anomaly Detection System, which learns from the previous attack and based on the knowledge gained, it mitigates future attack by crosschecking the behavior of the attack in its database. The reactive approach is a much easier method compared to the proactive method [1]-[3].

This paper highlights the security advantage of the reactive security approach in data security in a mobile wireless network and discusses data security in wireless networks. Section two discusses the proactive approach to data security and common attacks known to data in wireless environment. Section three discusses reactive approach to data security and different security mechanisms to ensure data security in wireless network environment. Section four describes topics on cryptography algorithms for data security while section five draws a conclusion on the reactive approach security and concludes research on data security in wireless networks.

2. Data Security

In securing data in the Information Technology environment, more than one method or mechanism is usually applicable to provide availability, integrity and confidentiality. Data communication over public networks should be encrypted using a good encryption algorithm and also a two-authentication method that would only give access to the right user, biometric approach can also be utilized as an authentication method. In data security, these services need to be put in mind (**Table 1**).

The Wired Equivalent Privacy (WEP) design is met for securing wired LAN by encryption which uses the Rivest Cipher 4 (RC4) algorithm encrypting messages with a shared key and using a two-side data communication that is the sender and the receiver [3] [4]. Data in broadcast or transmission is also prone to threats and they can be manipulated and compromised before it gets to its intended destination. In this kind of environment, 1) Data confidentiality and Integrity must be strong, and there should also be protection for replay messages, this can be achieved by using a cryptographic tool that has the replay protection techniques available. 2) Mutual Authentication, which provides a medium for users communicating to authenticate their identity, and subsequently

Table 1. Handling data security issues.

Objective	Technique
Confidentiality (privacy)	Symmetric/Private Key Cryptography
Integrity (has not been altered)	Asymmetric/Public Key Cryptography
Authentication and Non-repudiation (who created or sent the data)	Hashing Algorithms
Data Hiding	Steganography

a key combination is integrated and flexible authorization policies with secured access can be deployed to restrict users. 3) Availability which is also an important measure in data security, the network should be able to stop attackers form shutting down or manipulating the connectivity of the entire system on the network, if this is done appropriately it could prevent denial of service attack DoS or it can mitigate it. The WiFi Protected Access (WPA), also utilizes the RC4 for data encryption in a wireless network, but it also adopts a Temporal Key Integrity Protocol (TKIP) for its confidentiality. In detecting replay packets or messages in WPA, a sequence mechanism is used to increase the sequence number of each message or packet [4] [5]. The WPA improved authentication methods are Pre-Shared Key (PSK), which authenticates the connected users with a 128-bit encryption key and a distinct 64-bit Message Integrity Code (MIC) which is gotten from the PSK. Also, the IEEE 802.1X and the Extensible Authentication Protocol (EAP) which can be provide a stronger authentication [4]-[6]. The IEEE 802.11i provides an improved MAC layer security, provides authentication protocols, key management protocols, and data confidentiality protocols. Another technique is the use of a Closed System Authentication which hides the SSID broadcast [4]-[6]. This only gives access to users who know the SSID of the network to gain access to the network and join. Other methods to secure a WLAN outside the MAC layer such approach are:

- Physical Layer approach, choosing a good antenna, K and positioning can cut the rate at which signal is lost or leaked, thereby improving security in the network [6] [7].
- RF firewall design which help to protect the WLAN [7] [8]. This requires the 802.11 to be modified in the physical layer.
- IPsec, SSL and SSH are also different approach to securing network connection.

3. Mechanisms for Data Security

Protecting confidential data either in broadcast, transmission or at the intended destination, requires data encryption which is one of the most used mechanism for protecting or securing data in wireless networks.

3.1. Encryption

This is a process of securing data that is to be transferred between computers. The data needs to be scrambled in a way that it cannot be read without having the right code or key to decode the data [9]. If the message seem hard to break that means the security system is very secure. As shown in **Figure 1**, a common use of encryption and decryption techniques; in the figure, an unsecured message which is the (Plain Text) is encrypted using an encryption techniques that made the message unreadable (Cipher Text) without having the right decryption code or key. The message is sent over the network and the receiving end decrypts the message with the right key to view the content. In securing data, the encryption procedures are categorized into two which is Asymmetric and Symmetric encryption techniques. These techniques depends on the type of security key that is been deployed to encrypt or decrypt the data that was secured.

In general, an RBF network can be described as constructing global approximations to functions using combinations of basic functions centered around weight vectors. In fact, it has been shown that RBF networks are universal function approximators. Practically, however, the approximated function must be smooth and piecewise continuous. Consequently, although RBF networks can be used for discrimination and classification tasks, binary pattern classification functions that are not piecewise continuous (e.g., parity) pose problems for RBF networks Thus, RB The RBF network used in this work is given in **Figure 1**. It consists of an input layer, one hidden layer and an output layer.

3.1.1. Symmetric Encryption

This method of encryption give the sender and the receiver the right to set and agree on a shared key, that would be used in encrypting and decrypting the message or data that is to be sent. Afterwards they use the shared key they decided on to encrypt and decrypt their message, this is shown in **Figure 2**, where an assumption of Node A and Node B first agree on the system of encryption (cryptosystem) then they move forward to agree on the shared key for encryption then Node A encrypts the message with the key and send over the network, while Node B decrypts the message with the same key to read the actual information.

One of the drawbacks of the symmetric encryption is the means of sharing the secret key between the two nodes that are involved. The whole cryptosystem would fail if the secret key is known by a third party, then it is no longer secret [9] [10].

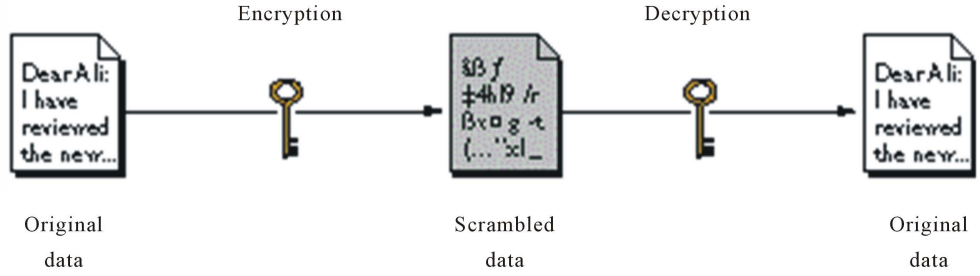


Figure 1. Data encryption.

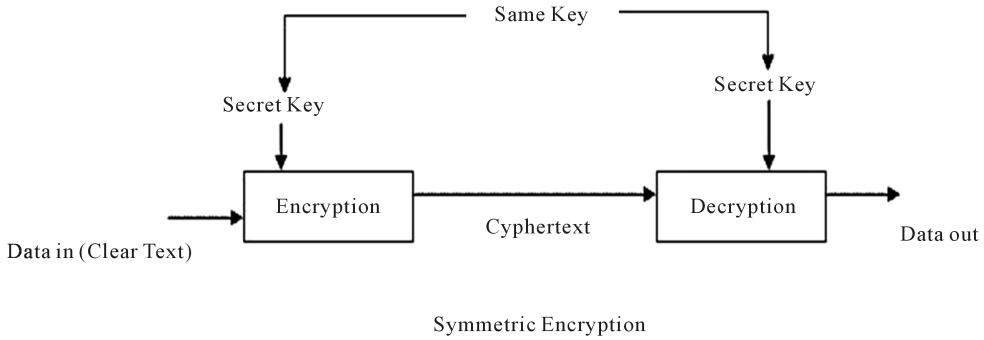


Figure 2. Symmetric encryption.

3.1.2. Asymmetric Encryption

In this type of encryption, two types of keys are used instead of one shared key compared to symmetric encryption method. That is for example a data is encrypt using KEY1 only KEY2 can decrypt and vice versa. This is because those are the two keys that was created for the encryption and decryption purpose. The public and private key can also be used, the Public Key Cryptography (PKC), the first key is made know to the public (which is the key for encrypting the data) while the private key is only know to the destination user (the one used for decrypting the data). **Figure 3**, depicts the process of the asymmetric encryption between node A and node B.

In Asymmetric encryption as illustrated in **Figure 3** with an assumption of data exchange between Node A and node B;

1) Node A and Node B agree on a cryptosystem.
2) Node B sends its public key to Node A.
3) Node A encrypts the message using the agreed public key (Cipher) and Node B's public key.
4) Node B decrypts the coded message using its private key and the agreed cipher from 1.

Asymmetric encryption techniques are slower than symmetric encryption techniques; this is because they asymmetric encryption techniques need more computational processing power to carry out its process [10] [11]. To fix this a hybrid system is usually advised, using the asymmetric encryption method to share the keys while the symmetric method to transfer data between Node A and Node B.

Table 2 shows the final comparison between Symmetric and Asymmetric key. This comparison covers different classifications.

4. Major Classification of Data Chiper

BLOCK CIPHER: The data encryption and decryption method used is in a block form, whereby the sender divide the plain text into blocks of plain text and it is inputted into the cipher system which in turn generated blocks of cipher text that would be send over the network to the desired destination. The block cipher have different types that are used such as: ECB (Electronic Codebook Mode), CBC (Chain Block Chain Mode), and the OFB (Output Feedback Mode) [11].

ECB: This form or block cipher, where the data blocks are encrypted and generated directly to form its corresponding ciphered blocks as shown in **Figure 4**.

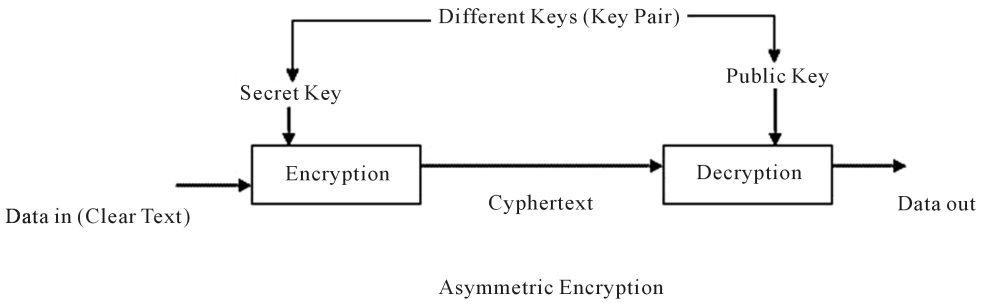


Figure 3. Asymmetric encryption.

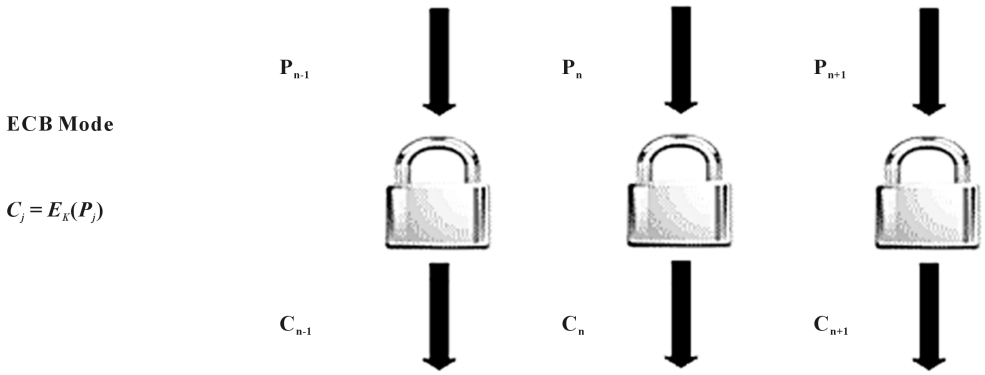


Figure 4. Block chiper: ECB mode.

Table 2. Comparison of symmetric and asymmetric algorithm.

Symmetric key encryption algorithm	Asymmetric key encryption algorithm
Simple Encryption/Decryption process	Process is Complex
Single Key—Private	Pair of Keys; Private is secret & Public is published to the world
Requires less processing Power & Time	More
Secret Key Management is difficult	Easy Management and maintenance

CBC: This makes use of the previous cipher block in the current cipher block, forming an encryption-chain process.

OFB: This works more like a stream cipher that uses plain text, where the encryption key that is used on current steps or process depends on the encryption key that has been used before [9]-[11].

STREAM CIPHER: The stream cipher consists of two components: a key stream generator and a mixing function. The stream cipher processes a data bit by bit.

The stream cipher is in two forms:

Synchronous Stream: this form of stream cipher, the cipher key stream generator is dependent on the base key used for encryption, this is shown in **Figure 5**; how the synchronous stream works, where the sender uses only the shared base key to encrypt the stream that is going out, while the receiver uses the same shared key to decrypt the key. The downside to this method is that if the key is known by a third party, the whole system is compromised.

Self-Synchronizing Stream Cipher: In this method, the key that is been used at a point or instant depends on the states of the cipher text bits. This method is slower than the synchronous stream method, but it is more secured. **Figure 6** shows its process of encrypting and decrypting of data.

The speed and simplicity of the stream cipher makes it more preferred compare to the block cipher, but the block cipher is more secured, so the block cipher is recommended [11] [12].

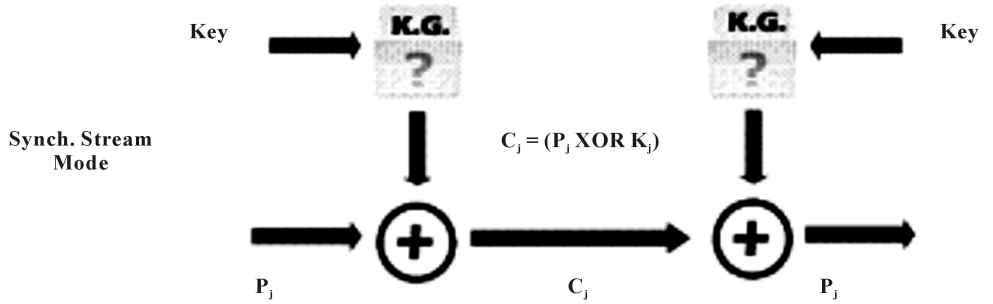
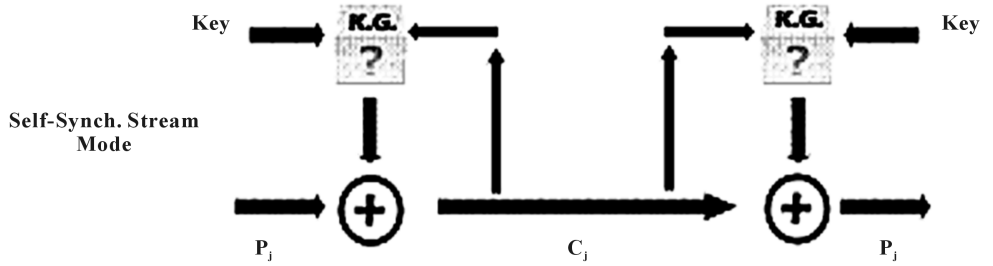


Figure 5. Stream chiper: simple mode (synchronous system).



$C_j = (P_j \text{ XOR } K_j)$

$K_j = f(C_j)$

Figure 6. Stream chiper: Self-synchronizing stream chipper.

5. Hash Algorithms

Hash algorithms function by converting data of random length into a smaller fixed length, this is commonly known as a message digest [12]-[14]. These types of algorithms are considered one-way functions. The generated output varies, making them very efficient when it comes to detecting alterations that might have been made to a message. Hash algorithms are often generated by the DES algorithm to encrypt online banking transactions and other communications where messages can't afford to be corrupted. In **Figure 7**, the public key is available although it can be distributed alongside the message, although the private key is secret and it is never included in the message. A digital signature it created and is verified by the asymmetric public/private key pair for authentication purposed. Then the sender signs the message content and adds his private key to the message and sends the message with the digital signature that was created earlier to the corresponding receiver or recipient. The digital signature is verified by the receiver with the sender's public key.

6. Proactive Approach for Data Security

The fact that security threats and risks are apparent in information technology, some threats might be successful while other might not be. The main view of the proactive security is that it reduces the impact of successful attack on the system and prevents loss of data or information while the system is still operational and secure. Proactive security approach in an organization for example, allows the organization to manage their security infrastructure and the values those infrastructure delivers [12]-[14].

In proactive security, 1) The redemption efficiency is identified proactively and also maximized, that is the weakness of the system is exploited so as to provide a good proactive security agent for future attacks. 2) proactive security access the real impact of a potential risk by tracing the paths of critical and non-critical information systems. 3) proactive security also assign security resources intelligently in order to fully focus on critical risks while the system is still operational, this helps to minimize or reduce interruptions of business time.

As discussed earlier in the proactive security approach, it anticipates threats behavior, prevent threats or attacks from occurring in the future. The proactive security system is a continuous learning system.

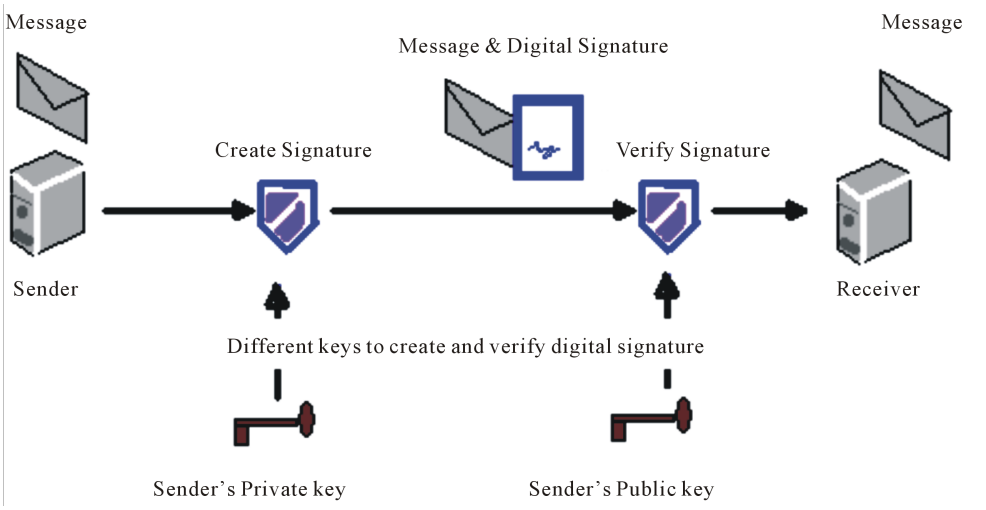


Figure 7. Hash algorithms.

From **Figure 8**, the proactive system is responsible for risk assessment definition of policies, implementation of proactive measures, updating infrastructure, and vigilant monitoring.

1) Risk Assessment: The proactive system assesses internal and external risk, so as to quickly create a preventive measure if it occurs. This uses a lot of resources because it creates a possible scenario before it happens and also creates a reactive solution to it.

2) Policies Definition: It defines security policies of the network due to its continuous learning capabilities.

3) Implementation of Protective measure: The proactive security system implements the following measure.

- Access Control: This requires both the authorization and authentication process.
- Scanning: It scans the traffic on the network for potential risk scenario and also the stored data traffic is scanned and protected. This is because access would be granted to data stored remotely over the network. The scanning protective measures utilizes recognizable patterns to identify virus threats and attacks on the network.
- Cryptography: This enables the secure communication between nodes in the network, secure electronic commerce for online transaction, and securing data. With this the transaction between the organization and customers would be secured [14]-[16].
- Network Perimeter Defenses: this creates a security measure around the full network.

4) Updating Infrastructure: This include the update of various software such as: Application software, monitoring tolls, virus definition, attack signature, and access control lists (ACL) [16]-[20].

5) Vigilant Monitoring: This monitors the system for threats and attack signature. The proactive system is responsible for monitoring the perimeter defense mechanisms, network patterns, anomalies, advisories and user activities.

7. Reactive Approach for Data Security

The reactive approach distinguishes itself from the proactive approach by being responsible for securing data after an attack or during an attack. The proactive method of security cannot necessarily be deployed without the reactive method that handles the risk afterwards. In reactive security some measures are put in place like; disaster recovery plan, switching to alternate systems in other locations, re-installation of OS and application if a system is critically compromised [21] [22].

These set of reactive response towards an attack can also be implemented further in the proactive method [23]-[27].

The reactive security measures are different from that of the proactive security measures; this is because the reactive measures are deployed after or during an attack. From **Figure 9**, the reactive security measures system is responsible for; security incident, post-mortem analysis, recovery measure, taking steps to prevent same attack from happening again [28]-[30].

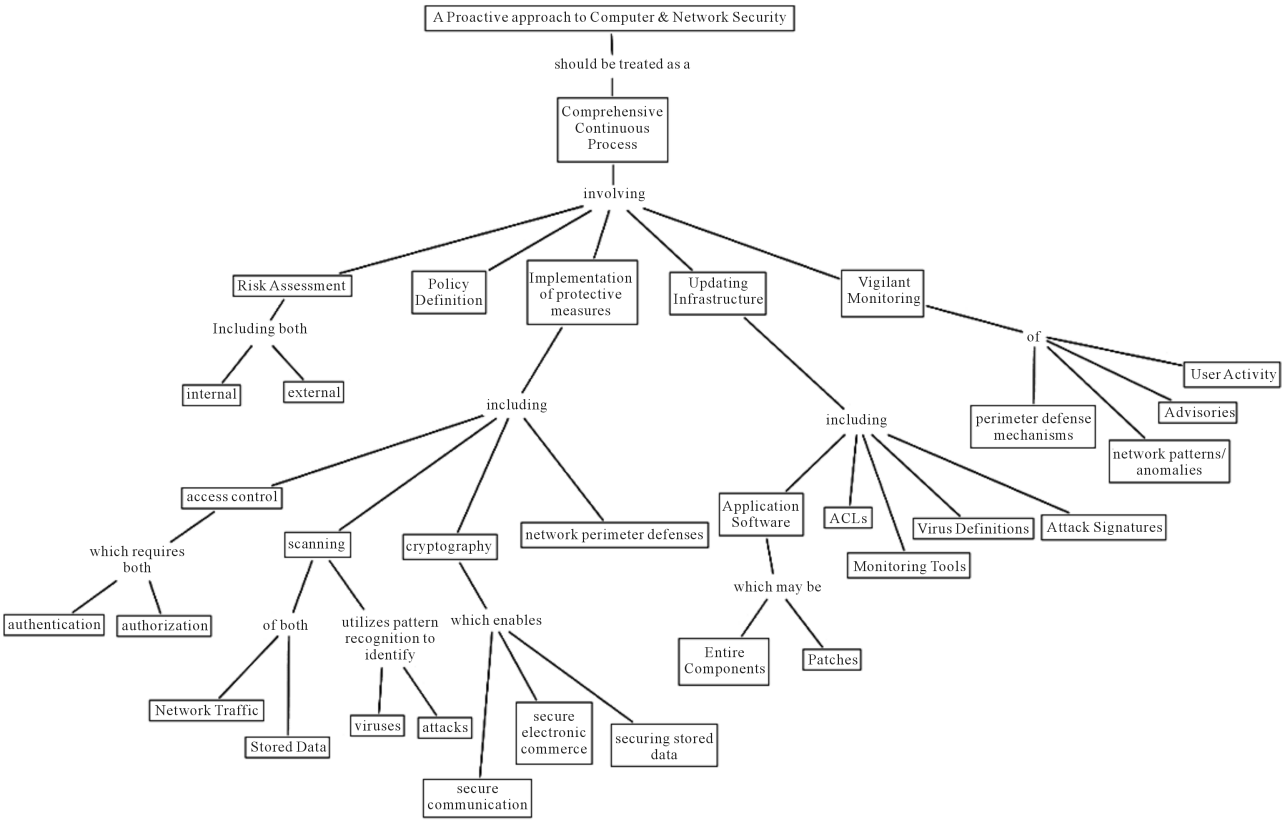


Figure 8. Proactive approach architecture.

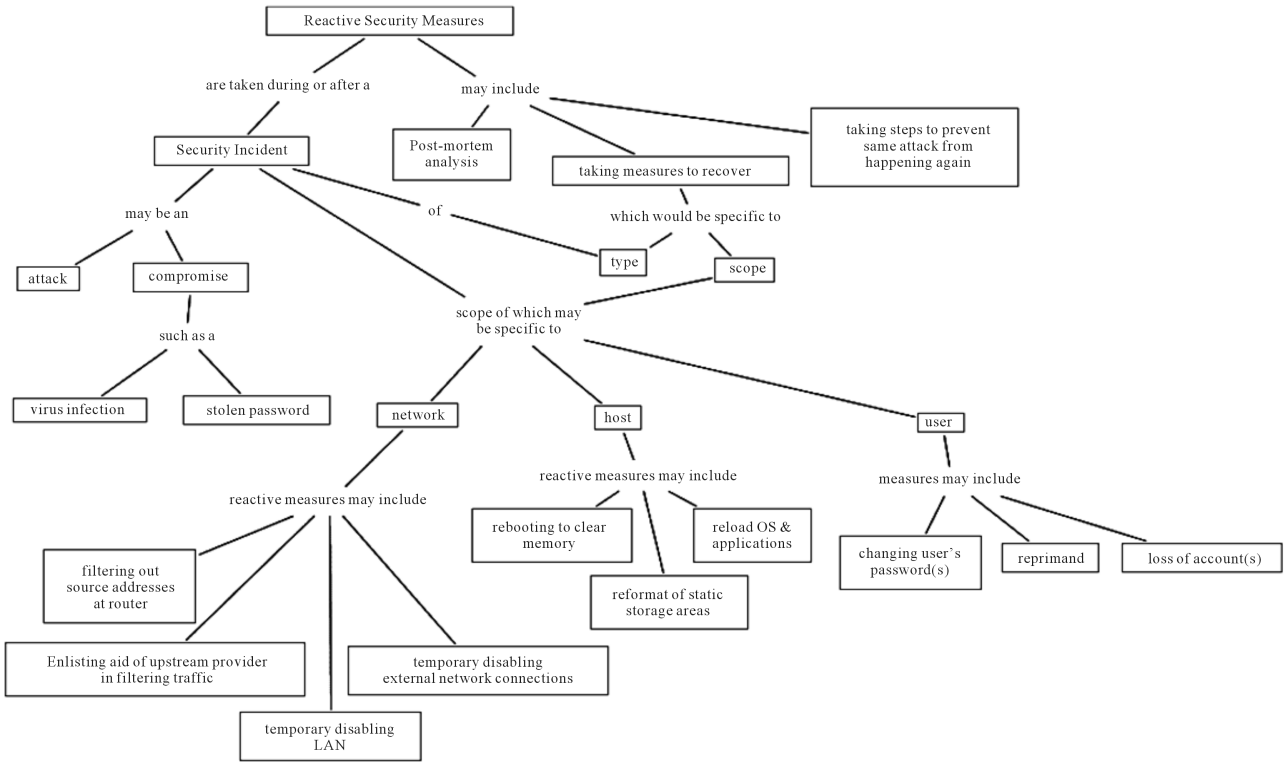


Figure 9. Reactive approach measures.

1) Security Incident: The incident may be an attack or a compromise such as a virus infection, or a stolen password. In such cases a quick reactive measure is taken to disinfect the file or system if it's a virus attack and restrict access or cut off users from accessing the corresponding files or system in the stolen password scenario.

The scope of the security incident may change to network, host or user.

- Network: If the network is faced with threats or an attack, the reactive security system will implement the following; filtering out the source address from the router, enlisting aid of upstream provider in filtering traffic, disabling the LAN temporarily and also other external network connection.
- Host: If the host is attacked the reactive measures may include: rebooting to clear memory, reformat the static storage areas, and reload the OS and other application.
- User: In the case of the user, the reactive security system measures may include: changing users password(s), reprimand, loss of account(s).

Reacting to dynamic environment resulted to reactive architecture, where reactive systems obtain their intelligence from the interactions they have with their environment. In the reactive architecture, there's a specific module that is responsible for starting up a direct reaction in response to a specific situation that occur in the environment [31] [32]. There is more than one module in the system, if one of the modules fails due to any reason, other modules continue their task. This causes the fault tolerance system of the reactive system to be robust [31] [32]. Variety of researches conducted different types of researches in the literature to secure Wireless networks however due to the nature and vulnerable infrastructure of wireless networks, different mechanisms forced reactive data security approaches to become more popular [31] [33].

8. Conclusions

This paper has carefully highlighted reactive security system and how they work. The reactive security system does not observe attacks like the proactive; it looks for the best way to secure the system. The deployment of the reactive security system or measures in either during or after an attack, it depends on the state of the attack. In this paper, we saw that in the reactive architecture the system has more than one module in its corresponding system, if one module goes bad, others will continue to function. This is like an anomaly detection system that detects threats and attacks by continuous learning. The reactive system is good in solving threats or tries to recovery and restricts attacks coming from network, host, or user region in the system.

In data security, it is best to use more than one security measure. In this paper, the proactive security mechanisms is designed to observe ad anticipate threats and or attacks, while the reactive is for recovering data and the state of system under attack or after the attack. Much research has not been done in this area of data security. Our future work would be conducting a comparative and performance evaluation study on the reactive security system over the proactive security system.

References

[1] Barth, A., Rubinstein, B.I.P., Sundararajan, M., Mitchell, J.C., Song, D. and Bartlett, P.L. (2010) A Learning-Based Approach to Reactive Security. *Proceedings of the* 14*th International Conference on Financial Cryptography and Data Security* (*FC'*10), 192-206. http://dx.doi.org/10.1007/978-3-642-14577-3_16

[2] Sari, A. (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. *International Journal of Learning and Development*, **2**, 18-30. http://dx.doi.org/10.5296/ijld.v2i2.1371

[3] (2003) Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley.

[4] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[5] IEEE P802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, April 2004.

[6] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[7] (2005) Bulletproof Wireless Security: Gsm, Umts, 802.11, and Ad Hoc Security (Communications Engineering). Newnes.

[8] Lynn, M. and Baird, R. (2002) Advanced 802.11 Attack. Black Hat Briefings.

[9] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306

[10] Bonde, J. (2011) Wireless Security, University of Minnesota UMM CSci Senior Seminar Conference Morris, MN.

[11] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[12] Hardjono, T. and Dodeti, L.R. (2005) Security in Wireless LANS and MANS. Artech House Publishers, London, 243-250.

[13] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[14] Schneier, B. (1996) Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second Edition, John Wiley and Sons, New York.

[15] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education*, **2**, 1-6.

[16] Marshall, T. (2001) Antennas Enhance WLAN Security. Byte Articles. http://www.trevormarshall.com/byte_articles/byte1.htm

[17] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18. http://dx.doi.org/10.14738/tmlai.25.430

[18] Josyula, D. (2006) Reactive Architectures. Dissertation, Department of Computer Science, University of Maryland. http://www.cs.umd.edu/~darsana/papers/dissertation/node151.html

[19] Chiornita, A., Gheorghe, L. and Rosner, D. (2010) A Practical Analysis of EAP Authentication Methods. 9*th Roedunet International Conference* (*RoEduNet*), 31-35.

[20] Hausken, K. (2006) Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, **8**, 338-349. http://dx.doi.org/10.1007/s10796-006-9011-6

[21] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[22] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[23] Sari, A. and Çağlar, E. (2015) Performance Simulation of Gossip Relay Protocol in Multi-Hop Wireless Networks. *Social and Applied Sciences Journal*, **7**, 145-148.

[24] Sari, A. and Mahmutoglu, H. (2013) Potential Issues and Impacts of ICT Applications through Learning Process in Higher Education. *Procedia—Social and Behavioural Sciences*, **89**, 585-592. http://dx.doi.org/10.1016/j.sbspro.2013.08.899

[25] August, T. and Tunca, T.I. (2006) Network Software Security and User Incentives. *Management Science*, **52**, 1703-1720. http://dx.doi.org/10.1287/mnsc.1060.0568

[26] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. In: *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN*'13), ACM Press, New York, 454-456. http://doi.acm.org/10.1145/2523514.2523586 http://dx.doi.org/10.1145/2523514.2523586

[27] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. *Proceedings of the Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*, Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[28] Fultz, N. and Grossklags, J. (2009) Blue versus Red: Towards a Model of Distributed Security Attacks. *Proceedings of the* 13*th International Conference on Financial Cryptography and Data Security*, Accra Beach, 23-26 February 2009, 167-183. http://dx.doi.org/10.1007/978-3-642-03549-4_10

[29] Sari, A. (2015) Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, Hershey, 66-94. http://dx.doi.org/10.4018/978-1-4666-8345-7.ch005

[30] Flegel, U. (2012) Reactive Security. *Information Technology*, **54**, 51-52.

[31] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of*

Communications, Network and System Sciences, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[32] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

[33] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. *Proceedings of the International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582. http://doi.acm.org/10.1109/TAEECE.2013.6557339

Int. J. Communications, Network and System Sciences, 2015, 8, 578-596
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813052

Scientific Research Publishing

Challenges of Internal and External Variables of Consumer Behaviour towards Mobile Commerce

Arif Sari[1], Pelin Bayram[2]

[1]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
[2]Department of Business Management, Girne American University, Kyrenia, Cyprus
Email: arifsari@gau.edu.tr, pelinbayram@gau.edu.tr

Received 25 August 2015; accepted 15 September 2015; published 30 December 2015

Abstract

The Mobile Commerce (m-commerce) becomes very powerful tool in the competitive business markets. Companies started to use this technology to attract their customers and catch their attention. Usage of Mobile commerce applications spreaded around different countries and became very popular. Different communication protocols and security techniques are designed for business use of m-commerce. Mobile Commerce, likewise the e-commerce brought significant difference in the market. People start to use this technology by feeling the freedom of having transactions at anywhere and anytime. However, consumers face lot of difficulties while using this technology which is consumer-based or service provider based. This research exposes the impact of determinants that influences mobile commerce application users' attitudes by classifying and investigating the internal and external variables in a case study of Cyprus Research Centre.

Keywords

M-Commerce, Internal Variables, External Variables, Consumer Behaviour

1. Introduction

Technology never stops to advance, as our needs increase so those new innovations come up and easier ways for things to work that will bring about efficiency.

Mobile commerce (M-Commerce) like its grand-daughter of Electronic commerce, enhance business strategies and simultaneously make it easy for users to comply with. M-commerce involves the Electronic transactions between buyers and sellers using mobile communications devices such as cell phones, personal digital as-

How to cite this paper: Sari, A. and Bayram, P. (2015) Challenges of Internal and External Variables of Consumer Behaviour towards Mobile Commerce. *Int. J. Communications, Network and System Sciences*, **8**, 578-596.
http://dx.doi.org/10.4236/ijcns.2015.813052

sistants (PDAs), or laptop computers (Miller, 2010). This form of commerce is flexible, highly mobile, and extremely versatile, making it a popular model for some businesses, including companies which only do business electronically as well as consumers in the public.

In many different countries, M-Commerce became very popular and powerful tool for communication and data exchange. People use this technology for private and corporate proposes. Different mobile commerce applications serve for different sectors. Today's technology savvy people appreciated for this technology because of its significant difference. It brought lot of advantages into our life from many different perspectives. Instead of music, video and chatting purposes, M-commerce brought significant difference for transactions at train stations, cinemas, parking places etc.

Payments, admissions to events, interactive services and information services such as weather forecasts, traffic information, exchange rates etc. are some of the advantages that mobile commerce provides to consumers at anytime and anywhere.

However, consumers face a lot of obstacles while using this technology. Consumer behaviour and attitudes towards mobile commerce change rapidly, because of several reasons which cause of these obstacles. These obstacles may be environmental, or consumer related. This study concentrated on the particular region and conducted a survey to analyze the consumer behaviour towards mobile commerce applications.

The paper is structured by discussing Mobile Commerce and Challenges of Mobile Commerce in section. Section 3 explains the relationship between M-Commerce and Challenges of M-Commerce with different subsections by covering customer loyalty and trust issues in M-commerce activities. The research model formulation, the hypothesis testing, sampling, data collection and questionnaire design are explained in Section 3. The findings of the research are exposed in Section 4 with different frequencies. Section 5 elaborates the results of hypothesis testing and concluding the research.

2. Mobile Commerce and Challenges of Mobile Commerce

The higher competition between business companies and popularity of mobile is increased rapidly in the last decade. Because of the advantages of the mobile, such as eliminating the distances, removing the communication barriers and providing 7/24 service to everyone, it became very important for the software and system developer companies. Customer centred organizations give primary importance to its customers. In order to adopt this new technology to customers, companies try to develop new sources and new solutions such as developing ease of use programs, user-friendly interfaces and higher security opportunities for particular transactions. Today, the mobile Internet is emerging even faster, in part because service providers, content partners, customers and investors of these markets are leveraging lessons both nationally and globally, have made significant advances enable next generation data or wireless Web services and mobile "m"-Commerce. Researchers have broadly defined the Mobile Commerce (m-Commerce) as it involves an emerging set of applications and services people can access from their Web-enabled mobile devices [1]. As it is stated before, this technology providing 7/24 services to everyone different than the other technologies. This type of technologies can bring many advantages to country's economies and welfare. As a developing technology, additionally, m-Commerce is facing many difficulties and obstacles as an emerging market, particularly in Small Island Developing States (SIDS). The main characteristics of SIDS are stated by researchers in the literature which these states are coastal countries that share similar sustainable development challenges, including small but growing populations, with the limited resources and very sensitive to natural affects and changes [2]-[5]. They are also vulnerable to external shocks like crises. Cyprus is one of these countries. For example, lack of standards, uncompleted infrastructure, cost and speed issues are main obstacles in Cyprus for m-Commerce. Because of these external factors which affect applicability and usability issues of m-Commerce, consumer behaviour and perceptions against m-Commerce becomes negative. In some of the developed countries, like US which also face some difficulty issues such as lack of standards, high mobile telecommunication costs and low speed, survey in the literature suggested that US consumers are not convinced they want or need mobile services and many think it is simply too complicated [6]. This is in contrast to other global markets in Asia and Europe where "to going online" means reaching for a mobile handset, not turning on a PC. In Korea, for example, reports which prepared by researchers suggest that one-third of all mobile phone subscribers use their handsets for m-Commerce activities [7]. This can easily explain us the popularity of m-Commerce services and mobile usage acceptance. As it is mentioned above, the mobile service provider companies working on development of usability and applicability

issues of m-Commerce services. But the new developments of mobile service providers may not have significant affect or changes on the customer perceptions alone. There are external and internal factors exist which may influence consumer behaviour and perceptions against m-Commerce services. The internal variables can be demographic or psychographic and external variables can be classified as social, cultural and technological. All these factors are important for to adopt consumers to use m-Commerce services. Usage of m-Commerce services have great amount of benefits for the local companies and businesses. The opportunity of 7/24 services availability gives advantages to customers to conduct transactions at anywhere-anytime and processing power which also gives an opportunity for business to offer services nationally, as well as globally. Several large companies abandon or scaling back country-based wireless efforts to focus on global markets. Additionally, carriers and content partners are still investing and bright spots exist. Several companies started to provide different services which are compatible and accessible for mobile devices. EBay recently launched a new service that lets customers bid more easily from mobile device. According to a Yankee Group report, the new service has the correct success factors-priced right, speed, and ease of use. Providing the compatible and accessible, faster and reliable services for consumer mobile devices brought a different dimension for business markets. Like e-Commerce, m-Commerce also represents a huge opportunity for businesses to connect to consumers through these mobile devices at any particular time. While a set of issues warrant attention, we focus on an area that has been largely neglected applicability, usability and security issues.

Many activities compete for a user's attention on the Web. There are different mobile services sending different information such as news, stories, weather information, exchange rate information, and alerts about stock prices, and notifications of e-mail services. The environment outside of the Web is fairly stable from day to day with wired e-commerce. Most of the places like offices, workshops and homes function with a good amount of predictability, even If they experience a huge amount of activity, and relatively consistent amounts of attention can be devoted to performing tasks on the computer. In m-Commerce world, conversely, there can be a significant number of additional people, objects, and activities vying for a user's attention aside from the application itself. The particular amount of attention a consumer can give to a mobile application will vary over time, and a user's priorities can also change unpredictably. For that reason, the circumstances under which m-Commerce applications and services are used can be significantly different from those for their desktop e-Commerce counterparts.

Moreover, in the m-Commerce environment, consumers and applications must deal with different and separate devices such as phones; handhelds, telematics, and this continue to shrink in size and weight. While this brings an opportunity and achieving high device portability, usability of the devices may suffer. Traditional mice and keyboards are being replaced with buttons and small keypads. But smaller screens are difficult to read and smaller devices are difficult to use with only one hand. The usage of mobile devices affecting from the external factors like noise level, weather and brightness. Difficulties of using mobile phones such as the lack of ease of use opportunities and user-friendly interface translate into waste of time or user frustration by the consumer.

Researchers have also stated that security is another serious challenging issue in the m-Commerce environments [8]. There are potential benefits in storing sensitive data, including medical, personal, and financial information on mobile devices for use by m-Commerce applications. But the vulnerability and mobility of these devices increases the risk of losing the device and its data. Moreover, the risk of data access by unauthorized parties makes positive user identification a priority. Different safety issues also arise when user activities starts to vary. In order to prevent unauthorized access and different precautions started to implement on this environment and sometimes, these precautions makes m-Commerce services inapplicable for the particular environment or area. For example, when designing the m-Commerce systems for automobiles, serious consequences can result if the application distracts driver from the traffic and diverts too much attention from the primary task of driving. So Web access or usage of m-Commerce applications in automobiles creates potential problems associated with browsing while driving. But in addition to this, such kind of problems may be solved by designing minimal-attention interfaces. As it is mentioned above, the dynamic environment may cause problems because of it's instability and context awareness systems may warn consumers for the particular events. New designs and flexible Input/Output systems may be developed to provide ease of use which will prevent mobile device limitations and usability. Lack of data sharing and data security may cause loss of customer trust against m-Commerce services system. In order to create customer trust against these services, security must be strengthening thorough new biometrics security systems, commonsense design and legislation of the entire system. Researchers have stated the potential challenges of m-Commerce in his previous studies. **Table 1** indicates some of these potential

m-Commerce challenges and potential solutions of these problems [9].

As it is shown in **Table 1**, there are varieties of challenges available for M-Commerce and potential solutions in contrast to these challenges. The one of the main challenge is that while there is a significant demand available in the market, there is a minimal attention for developing m-commerce application interfaces. The dynamic environment that leads both security and safety issues as vulnerable objects, different solutions proposed such as usage of biometrics and common-sense design with legislations.

While Mobile commerce (M-Commerce) is discussed and stated, it was compulsory to discuss the e-commerce first of all. For that reason, the previous section described the commerce briefly in order to clearly define the e-Commerce which is also known as "Electronic Commerce". In order to understand the importance and role of E-Commerce, we must differentiate the e-commerce and m-commerce from each other. Researcher has explained the e-commerce as a monetary transaction which conducted using the combination of internet and a desktop or laptop computer [10]. So it's clearly stated here, the need internet connection and computer is compulsory for usability of e-commerce. As long as e-commerce has relationship between m-commerce, the same or similar tools will be required as well. For the applicability of these systems, it's again the internet connection will be compulsory.

Mobile commerce has many similarities with e-commerce. It's kind of more developed and technological based partner of commerce family. Once the wireless or any other internet connection device take place in the system, and allows clients or users and provide freedom of movement, the name of the commerce becomes "Mobile Commerce". The basic milestone of the development of M-commerce started with Wi-Fi which is called Wireless Fidelity. For that reason, the researchers defined the mobile commerce as any transactions using a wireless device that result in the transfer of monetary value in exchange for information, goods or services [11]. This definition is very similar to the e-commerce definition which is done by the researcher [10]. The role of computer or laptop is completely taken by mobile devices such as PDA's, or mobile phones. The source of communication which is provided for the data transmission is also same which is "Internet" but the devices is not switch or hub, and it's a new technology which is wireless telecommunication network devices, wireless hubs, or wireless antennas that allows users to connect to internet at anywhere and anytime. The e-commerce websites are designed for e-commerce and could be accessed through combination of computer and internet. The clients were accessing to these websites through internet and computer, conducting a transactions. In the case of m-commerce, all these websites are designed and coded according to the some compatibility standards, so clients were accessing these websites through mobiles and doing all of the same processes likewise e-commerce. Once a client accessed to the website, and transaction conducted from the mobile and through a wireless connection media, this is called Mobile commerce process. Researchers have proposed a book and defined the mobile commerce as "a monetary transaction for goods and services conducted by a mobile device, an operating system specific to mobile devices and a mobile-dedicated infrastructure." [12].

Clients are using mobile commerce applications which are developed by software developers and connecting to the internet through their GSM operators. The clients browse and surf on the company websites, by using the software that is developed for mobiles.

Since the beginning of the section, we have tried to explain the e-commerce and m-commerce. It is mentioned on the above that, m-commerce is an extension or more developed and technological way of e-commerce. But on the other hand, it must be stated that, there are very basic differences between m-commerce and e-commerce which are use of communications protocols for transactions, types of internet connection and the connection media, the key enabling technologies, and development languages.

Table 1. M-Commerce challenges and potential solutions [9].

Challenges	Potential Solutions
Increased demands on attention	Minimal-attention interfaces
Dynamic environment	Context awareness
Mobile device limitations and usability	New and flexible I/O modalities
Security	Biometrics
Safety	Commonsense design and legislation
Social concerns	Societal norms and written laws

For example, while the m-commerce is giving freedom of movement to the clients, it requires Wireless Application Protocol (WAP) which is a key for enabling the m-commerce technology. Clients access to the internet through the WAP technology and access/browse the pages. All data and packet transmission from the wireless media provided through WAP. So the WAP becomes a communication standard for the m-commerce. But in e-commerce technology, we do not need the WAP technology to enable us to connect to internet. Instead of this, the computer use Hyper Text Transfer Protocol (HTTP) and standardize the pages using Hyper Text Markup Language (HTML) in order to browse/show pages by using internet browser. On the other hand, WAP requires Wireless Markup Language in order to standardize the formatting of pages and display them on the mobile devices.

Customer Loyalty and Trust in Mobile Commerce

The concept of trust has been studied in different disciplines ranging from business to psychology to medicine, and perspectives on it differ, but it can be loosely defined as "a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk" [13]. Business relationship would be nonexistent without trust, which is expressed in various business contexts such as laws, contracts and regulations as well as in company policy and personal reputations, and long term relationships. Once the customer trust is gained by the business, this situation becomes long-term relationship between the customer and business and it transforms to loyalty during the particular period of time. Not surprisingly, studies show trust also plays an essential role in successful Internet retailing [14]. Gaining customer trust in m-Commerce is a frustrating process, extending from initial trust formation to continuous trust development-but it can be done. Studies by researchers shows nearly all customers refuse to provide personal information to a Web site at one time or another, a majority because they lack trust in the site [15]. Most of these customers are still not comfortable with the concept of Web-based developments and the electronic medium itself. They are distrustful that e-Commerce can satisfy consumer needs unfulfilled in the bricks-and mortar business world, and they wonder whether e-Commerce is technologically feasible, and reliable. From this uncertainty point of view, it's a small step for customers to doubt the integrity of Internet vendors. Without social cues, and personal interaction such as body language, linguistics, the observation of other buyers, and the ability to feel, touch, and inspect products directly, customers can perceive online business and transactions as riskier in nature.

According to researchers [16], gaining consumer trust in m-Commerce world, which uses radio-based wireless devices to conduct business transactions over the Web-based e-commerce system, is particularly frustrating task because of its unique features. As it is stated about m-Commerce challenges on the previous paragraphs, mobile devices are terrifically convenient for anytime shopping, and offering various types of advantages both the consumers and businesses. But their small screens, low resolution displays and tiny multifunction keypads make developing user-friendly interfaces and graphical applications a challenge. Comparatively, mobile handsets are also limited in computational power, memory and batter life. Once it is considered that, m-Commerce is involved into the Wireless Networks; major limitations of these networks must be taken into consideration. These networks have difficulties of providing huge bandwidths and they have connection stabilities as well as function predictabilities. Also, relatively high operation costs, lack of standardized protocols and data transmitted wirelessly is more vulnerable to eavesdropping.

Various factors may influence the complex process of engendering customer trust in Internet shopping. These are the factors and variables that influence consumer behaviour such as internal-demographic, psychographic and external-social, cultural and technological variables. The consumer characteristics such as need, motivation, capacity and willingness, along with the seller characteristics such as ability, benevolence, and integrity, all play a role in Internet purchasing and m-Commerce usage behaviour [17]. Customer perception of security and privacy control, integrity, and competence, as well as third-party recognition and legal framework are important antecedents of trust in Internet shopping [18]. There are several other factors exist which may influence customer trust and trigger Internet shopping such as personal experience, familiarity, affiliation and belonging, transparency, factual signals and heuristic cues. **Table 2** indicates some of the factors which may influence consumer behaviour against m-Commerce and Internet shopping.

3. Research Model Formulation

There is a need for determination of variables in the hypothesis creation progress. The determinants that impact

Table 2. Factors influence consumer behaviour against internet shopping.

Category	Consumer Characteristics	Seller Characteristics	Consumer Perceptions	Consumer Perceptions for Corporate Branding
Factors	Need	Ability	Security	Personal Experience
	Motivation	Benevolence	Privacy Control	Familiarity
	Capacity	Integrity	Integrity	Affiliation and Belonging
	Willingness		Competence	Transparency
			Third-party recognition	Factual Signals and Heuristic cues
			Legal framework	

the hypothesis testing as internal or external should be classified and explained. This section explains the formulation of research model in details.

Figure 1 shows the general research model formulation. The impact of determinants which affects the mobile commerce customers is divided into two (2) categories of variables which are Internal and External variables. As it is shown below, internal variables are classified as demographic and psychographic, external variables classified as social, cultural and technological variables. In this study, two (2) hypotheses are formulated through the impact of internal and external variables towards the mobile commerce. The variables which mentioned above would be discussed clearly later sections of this study.

3.1. Formulation of Research Objectives and Hypothesis

To identify the impact of internal variables (demographic and psychographic variables) on consumer behaviour towards mobile commerce;

H1: There is a significant impact of internal variables (demographic and psychographic variables) on consumer behaviour towards mobile commerce

To identify the impact of external variables (social, cultural and technology variables) on consumer behaviour towards mobile commerce;

H2: There is a significant impact of external variables (social, cultural and technology variables) on consumer behaviour towards mobile commerce.

There are 4 different types of variables exist which are classified as, dependent, independent, moderating and intervening variables. In this research, some of these variables are shown and classified in **Figure 2**.

Figure 2 is showing the classification of the variables during the formulation of the hypothesis.

The variables which are classified under the Psychographic variables referring to any other attribute related to personality, lifestyle, values, interests or attributes. These factors consider various influences on a person's buying behaviour. Different lifestyle choices like parenting, exercise decisions, religion, marriage or health can greatly affect a person's requirements or preferences for certain products or services.

Technological Variables; was developed to measure and categorise consumers based on ownership, use patterns and attitude towards different technologies. A concrete example would be humanity's attitude towards the Internet. There are distinct differences between frequent Internet users and those who seldom use it. Most experienced Internet users are more affluent and tend to be more optimistic towards modern technology than those who are not as manifested by the number of online shoppers. Confident online shoppers are those who have been using the Web for quite sometime thus, making them feel safer compared to newly recruited Web users.

The behavioural variable of market segmentation groups consumers in terms of occasions, usage, loyalty and benefits sought. This is based on the way different consumers respond to, use or know a product or service. The variable of occasion simply means the occasion on which a product or service is consumed or purchased.

3.2. Range of Study and the Sample Selection

This study focuses the students of Research center in Cyprus. Students from different research departments are participated in this project. The total number of students who participated in this project is 100. The total population of the research center is approximately 971.

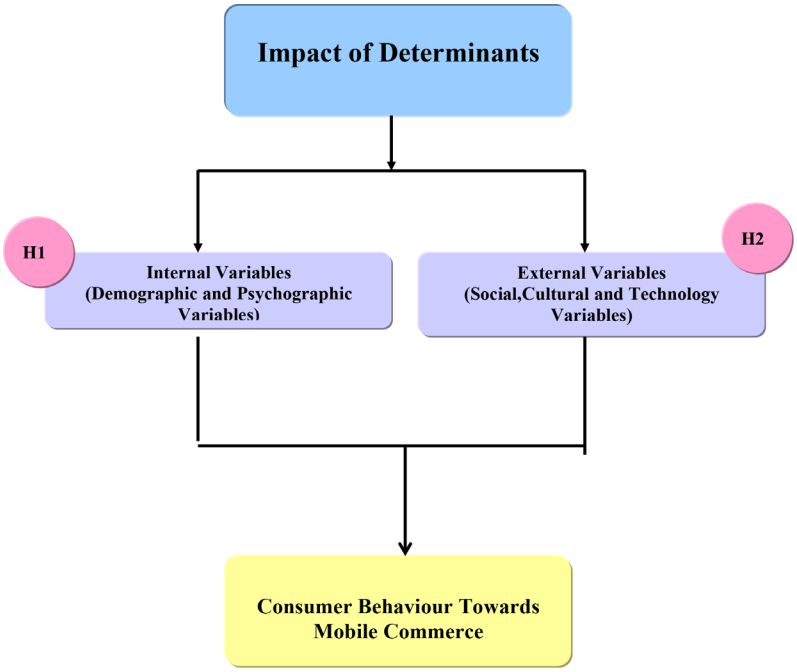


Figure 1. Research model formulation.

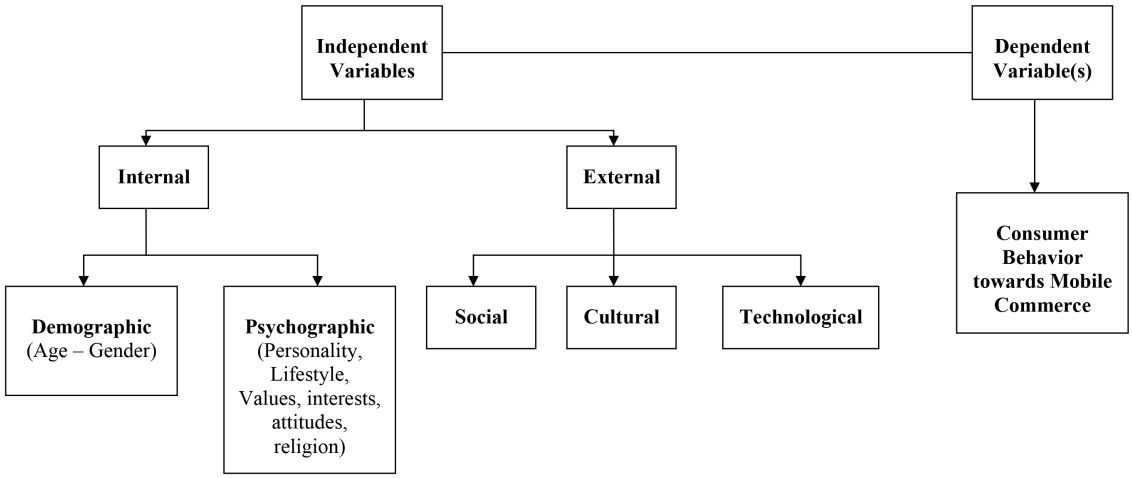


Figure 2. Dependent and independent variables classifications.

3.3. Data Collection

In this research, two different sources are used to accomplish the objectives of this study. The primary sources and the secondary sources.

3.3.1. The Primary Sources

The primary source for this research is the information collected through questionnaires. The information obtained from this source has provided statistics, which measure the students' behaviour against mobile commerce applications.

3.3.2. Secondary Sources

The secondary sources will be gathered from references and published books, journals and information available on the internet. Additionally, some data obtained from the particular websites from the Internet.

3.4. Sample Plan

The following sample units have been selected based on the following methods and the sample units ought to have requisite criteria to get selected for the study.

- Should be a student of Cyprus Research center.
- Should be registered to one of the programs at Cyprus Research center.
- The participants should be aware of the mobile commerce applications.
- The participants should be able to use mobile commerce applications.
- The participants should have a mobile device that is compatible to mobile commerce applications.

3.5. Sampling Technique

A simple random sampling has been used to select target respondents for this study. The students of Research Centre have been informed on the purpose of the study and the willing students participated in the study. Responders for the survey were randomly selected 100 individual people from Research Centre. The sample population include only students as well as those students who work outside as well.

3.6. Sample Size

The sampling size is used for this research study is One Hundred (N = 100).

3.7. Research Tools and Collection Instrument

The instrument used for collecting the primary data is questionnaire. The questionnaire is a structured questionnaire. Selective questions were asked and respondents just ticked appropriately. Open ended questionnaire was used for the pilot study and the result of the open ended questionnaire was used to formulate the closed end structured questionnaire.

3.7.1. The Questionnaires

The collection method used is hand delivery of the structured questionnaire to the respondents personally by the researcher of this study. This was done in order to ensure the respondents understand the questions before ticking appropriately. The structured questionnaire was also translated into Turkish language for easy understanding by the respondents.

Questionnaires are one of the most widely used social research techniques. The questionnaires will be utilized to gather information from subjects. This is to explore the impact of determinants on consumer behaviour against mobile commerce applications and mobile commerce as well. Researchers stated that “Questionnaire is one of the most widely used survey data collection techniques, because each respondent is asked to response to the same set of questions, it provides an efficient way of collecting responses from a large sample prior to quantitative analysis” [19].

There are two main types of surveys, questionnaire and interviews. The method selected for this research was the questionnaire. The questionnaire are classified into two types; those which are designed for self-completion in which the respondent complete the questionnaire themselves, and those which designed for assisted completion wherein the researcher asks the questions and fill in the questionnaire himself [20].

3.7.2. The Design of the Questionnaire

The contents of the questionnaires were mainly derived from the literature review. In addition, from some research and studies conducted in this field.

The questionnaire is developed in English but because of the student’s profile at Research Centre of Cyprus and as it is stated before; the questionnaire is also translated into Turkish. This action has granted two main factors for the questionnaire;

Firstly, helped in saving time spent with respondent to translate and explain the questionnaire elements. Secondly, it guaranteed the highest level of understanding of the questionnaire items and the ideal amount of freedom for answering.

3.7.3. The Questionnaire Contents

The questionnaire containing totally 10 questions. The first 3 questions were designed to gather main general

information of the respondents such as age, sex, nationality, occupation and monthly income. The question number four to question number eight containing the questions about the frequency of conducting mobile commerce transactions and measuring the frequency of usage of mobile commerce. Especially, question number six, is measuring the usage of particular mobile commerce transactions.

The last 2 questions were designed to examine the consumer's satisfactions and perceptions against mobile commerce applications and their recommendations about mobile commerce. The question number 9 is 5 point scale designed question and measuring the replies in five ranks. This question was measuring the actual reason of usage of M-Commerce by people. It also shows the personality, perceptions and the consumer behaviour against mobile commerce applications. The more details about this question are given in the "Findings" section of this study.

The questionnaire in the study was designed for the Bachelor students who are studying in any faculty and department of Cyprus Reserach Center. Single questionnaire was given to each respondent which containing the questions about his or her perceptions, and particular behaviour which determining the influencing factors of Mobile commerce usage. The questionnaire contained questions used to determine the demographic distribution as well as perceptions and behaviours of the respondents. **Question 1** was based on the age distribution of the respondents; Below 20, 21 - 30, 31 - 40, 41 - 50, and above 50 years. **Question 2** was based on the gender of the respondents; Male or Female. **Question 3** was based on the nationality of the respondent, Turkish Cypriot, Turkish, British and Others. **Question 4** was designed based on the occupation of the respondents, which could be; Student, Private, Business, Housewife. **Question 5** was designed based on the Monthly Income of the respondents in terms of Turkish Liras (TL) and which can be; Below 1000, 1001 - 2000, 2001 - 3000, 3001 - 4000 and above 4000. **Question 6** was based on the mobile different types of commerce transactions and it was aiming to find out the most frequently done mobile commerce transactions by the consumers. **Question 7** was designed to find out conducting the mobile commerce frequency of consumers which is limited with last 12 months time period and can be; Once, 2 - 4 times, 5 - 10 times, More than 10 times. **Question 8** is designed for to measure the amount of money spent on m-commerce transactions in terms of Turkish Lira and which can be; Below 50, 51 - 100, 101 - 150, 151 - 200 and Above 200. The **Question 9** is designed based on the "Five Points Likert" scale. The respondents were asked to rank their interests (against using mobile commerce services) using highly agrees as the highest and highly disagrees as the least. **Question 10** was designed for to measure the recommendation of mobile commerce by respondents to their relatives and friends which can be; Definitely Recommend, Somewhat recommend, No Comments, Do Not Recommend, Not at All.

3.7.4. The Questionnaire Responses

The questionnaire was targeting to all students at all faculties in Research Center. It was necessary to distribute the questionnaires to most of the departments of these faculties. The 100 questionnaires were been distributed, 100 of them collected, and none of the questionnaires rejected because of incompletion or as an unfilled.

3.8. Limitation of the Study

There are specific limitations exist for this research. These are:

- The data collected were purely based on knowledge, perception, feelings, attitude and opinions of the target respondents.
- The research would have the limitation like all the social science research does.
- The study had been conducted in Cyprus Research Centre and the results could not be generalized.

4. Findings

In this section the analysis of the survey will be highlighted and discussed. The mobile commerce service providers and applications developers keep conducting the researches to understand the customer profiles and analyze their needs in order to create better and secure mobile applications. But people perceptions differ and behaviour may vary depending on the time, place and corresponding action. The survey of this research shows the different perceptions of people, their actual reasons of usage of the mobile commerce applications, their problems with this technology and their recommendations. Additionally, each questionnaire is analyzed carefully, and consumer's viewpoints measured in this research. Moreover, people spending on mobile commerce, and their main reasons of usage of this technology became some of the major interesting outcomes of this study.

4.1. General Information about the Sample

This analysis is based on the data collected from 93 respondents. As it is mentioned before, responses from 100 respondents could succeed %100 and no unfilled-uncompleted questionnaires received. 100 respondents from different faculties and different departments of Cyprus Reserach Center. The demographic information includes nationality, age, sex, occupation and monthly income.

4.2. Age Group

With regard to the age, out of the total number of students in the sample, between 21 - 30 years old represent the largest proportion which is 92% (92 respondents) and 8% of respondents participated in this research project. There is no respondent participated in this project above 30 years old. **Figure 3** and **Table 3** shows the same information about the distribution of population in different ways.

Inference: From the **Figure 3**, **Table 3** and analysis, it can be inferred that majority of the respondents used for this study are below 30 years old. Only 8% of respondents are in the category of "Below 20" years old.

4.3. Gender Ratio

Table 4 shows that, there are totally 68 male respondents and 32 female respondents participated in this survey. **Figure 4** shows number of respondents participated in this survey in a chart model.

Inference: From the above analysis, it can be inferred that majority of the respondents used for this study are male.

Table 3. Age frequency of respondents.

Age	Number of Respondents	% of Respondents
Below 20	8	8%
21 - 30	92	92%
31 - 40	0	0%
41 - 50	0	0%
Above 50	0	0%
Null	0	0%
Total	100	100%

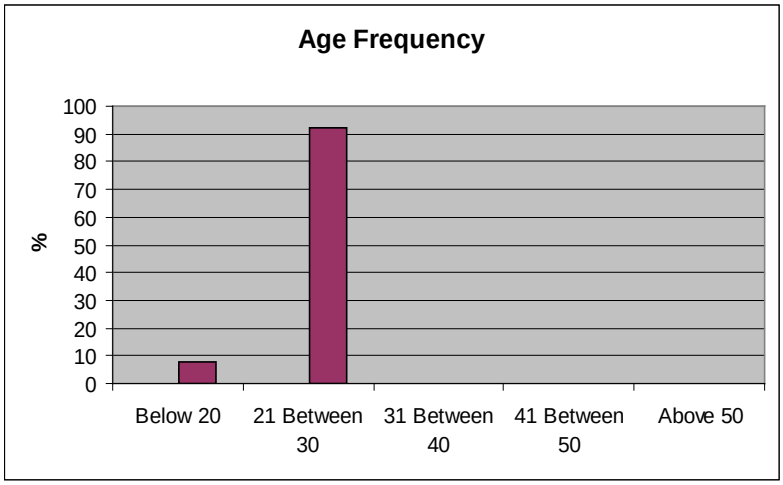


Figure 3. Age frequency of respondents.

4.4. Nationality Distribution of Respondents

The nationality distribution of the sample is given in **Table 5** and **Figure 5**. According to **Table 5**, there are totally 13 Turkish Cypriot respondents (13%), 50 Turkish respondents (%50), 0 British respondents (0) and 28 other's nationality holder's respondents (28%) participated in this survey.

Inference: According to the data gathered and analyzed above, it shows that majority of participants are Turkish and Other nationality citizens. The Turkish Cypriot citizens have the minority of contribution in this survey. There is no British citizen participant exist in this survey.

Table 4. Gender ratio of respondents.

Gender	Number of Respondents	% of Respondents
Male	68	68%
Female	32	32%
Null	0	0%
Total	100	100%

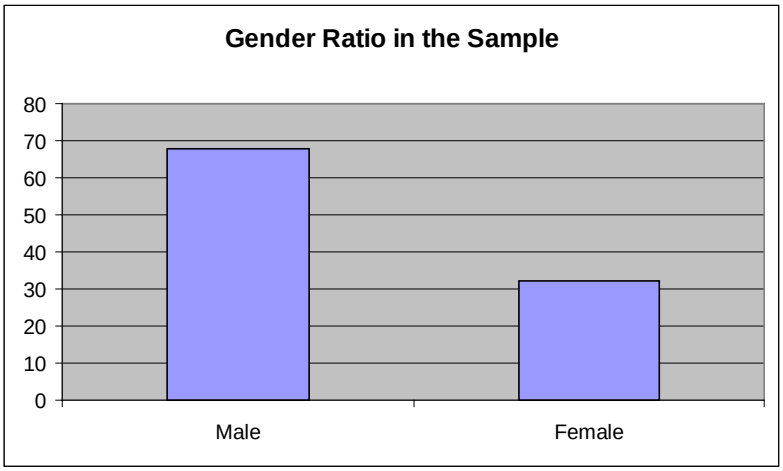


Figure 4. Gender ratios of respondents.

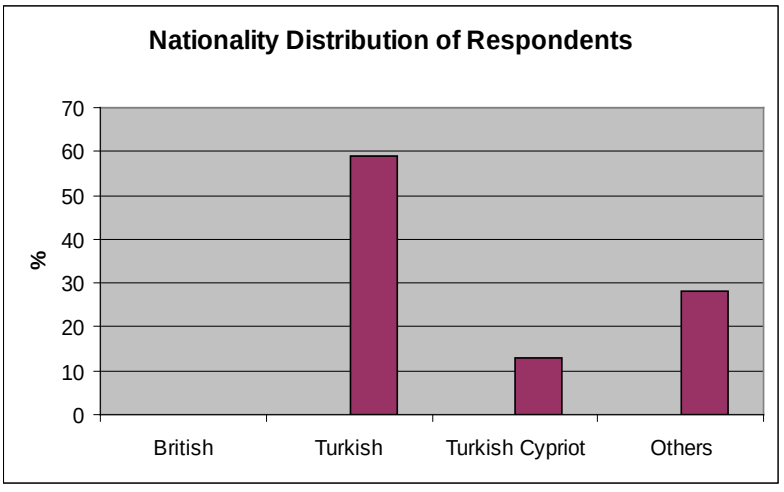


Figure 5. Nationality distributions of respondents.

4.5. Occupation of Respondents

In this analysis, it is found that the highest percentage of respondents is students. **Table 6** is showing the occupation of the respondents. According to **Table 6**, there are 100 (%100) of students participated in this research and there is 0 (0%) of workers or housewife attended or involved in this survey.

Inference: **Figure 6** and **Table 6** show the distribution of occupation among participants. According to these results, it can be said that, all participants who participated in this survey was students.

4.6. Income Ratios of Respondents

The data shown below on the. **Table 7** is showing the Monthly income of the respondents who participated in the survey. According to **Table 7**, there are 100 (%100) of respondents participated in this research who had a salary of below 1000 TL and there is 0 (0%) of respondents participated who has salary more than 1000 TL in this survey.

Table 5. Nationality distribution of respondents.

Nationality	Number of Respondents	% of Respondents
Turkish Cypriot	13	13%
Turkish	59	59%
British	0	0%
Others	28	28%
Total	100	100%

Table 6. Rate of occupation in the survey.

Nationality	Number of Respondents	% of Respondents
Student	100	100%
Private	0	0%
Business	0	0%
Housewife	0	0%
Total	100	100%

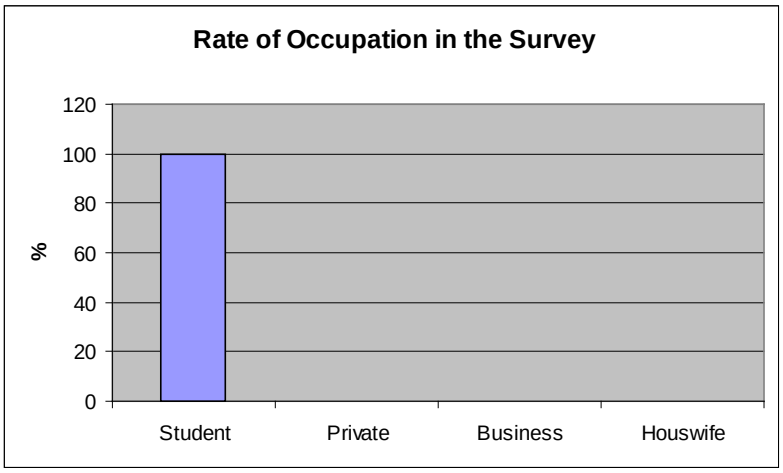


Figure 6. Rate of occupation in the survey.

Table 7. Income ratios of respondents.

Income (TL)	Number of Respondents	% of Respondents
Below 1000	100	100%
1001 - 2000	0	0%
2001 - 3000	0	0%
3001 - 4000	0	0%
Above 4000	0	0%
Total	100	100%

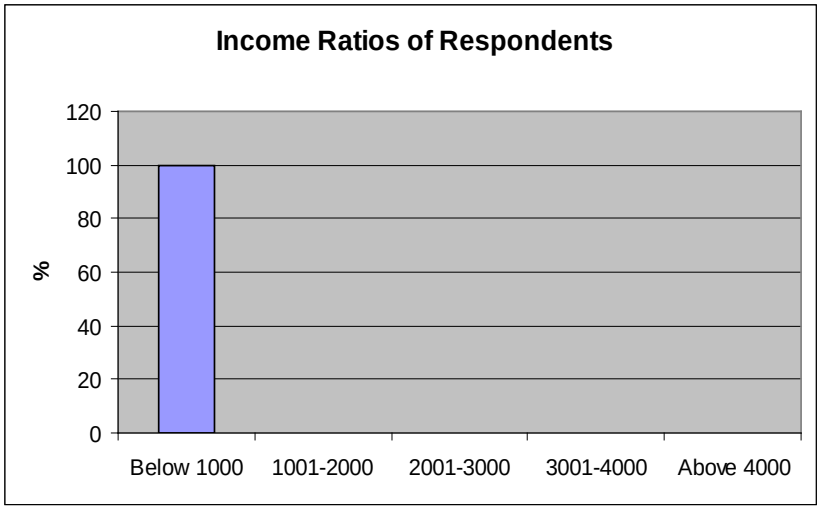


Figure 7. Income Ratios of respondents.

Inference: Figure 7 and Table 7 show the distribution of income ratios among participants. According to these results, it can be said that, all participants who participated in this survey has a monthly income of less then or equal to 1000 TL.

4.7. Types of Mobile Commerce Transactions by Respondents

Table 8 is showing the types of M-Commerce transactions conducted by the respondents. It is important to state that, majority of respondents who participated in this research prefer interactive services such as chats and games (79%). Most of the respondent mentioned about the "facebook" and "twitter" web addresses at the time of distribution of the questionnaire. Only a few respondent selected ringtones which is equivalent to 10% (10 respondents), 2% of respondents (2 respondents) and 5% (5 respondents) selected Music and Content which showing that they involved into m-commerce applications and services for this case.

None of the respondents involved into the services of mobile commerce such as, admissions to events, parking, or others. The respondents also mentioned that, they could not involve into these services just because of the unavailability of these services, or they could not find it beneficial for themselves. Figure 8 is showing this distribution clearly.

Inference: The stated analysis and table-figure above shows that, respondents who participated in this survey, prefer social activities, such as chatting or web-forums. This also can be considered as one of the difference because of the respondent's age group and business. On the other hand, other selections which are not selected by the respondents should also be considered carefully.

4.8. Frequency of Mobile Commerce Transactions by Respondents

Table 9 below is showing the frequency of m-commerce transactions done by respondents for the last 12 months. The majority of respondents (45%) replied as they have conducted a transaction more than 10 times for last 12 months. 33% of respondents replied as 5 - 10 times, 18% of respondents replied as 2 - 4 times and 4% of respondents replied as they have conducted a transaction just once.

Inference: According to the analysis, it can be said that, majority of respondents have conducted mobile commerce transaction for last 12 months. However, there are other respondents exist, who did not conduct this much of transaction for different reasons which they have not stated. **Figure 9** is showing the frequency in a bar chart model.

Table 8. Types of m-commerce transactions done by respondents.

Type of Services	Number of Respondents	% of Response
Ringtones	10	10%
Screen Savers	4	4%
Music and Video Content	5	5%
Interactive services, such as chats, games etc.	79	79%
Information services, such as weather forecasts, traffic information etc.	2	2%
Admissions to events	0	0%
Parking	0	0%
Other	100	100%

Table 9. Frequency of m-commerce transactions done by respondents for last 12 months.

Frequency	Number of Respondents	% of Respondents
Once	4	4%
2 - 4 Times	18	18%
5 - 10 Times	33	33%
More Than 10 Times	45	45%
Total	100	100%

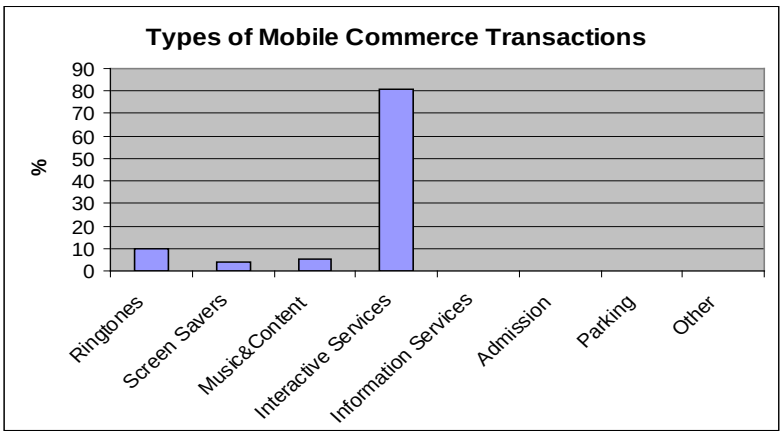


Figure 8. Types of m-commerce transactions done by respondents.

4.9. Amount of Money Spent on Mobile Commerce Applications

Figure 10 and **Table 10** showing the amount of money spent on Mobile commerce applications for last 12 months by the respondents. According to this data, 63% (63 respondents) spend less than 50 TL, 28% of respondents spend 51 - 100 TL, 9% of respondents spend 101 - 150 TL and 0% of respondents spend more than 101 TL on the mobile commerce transactions.

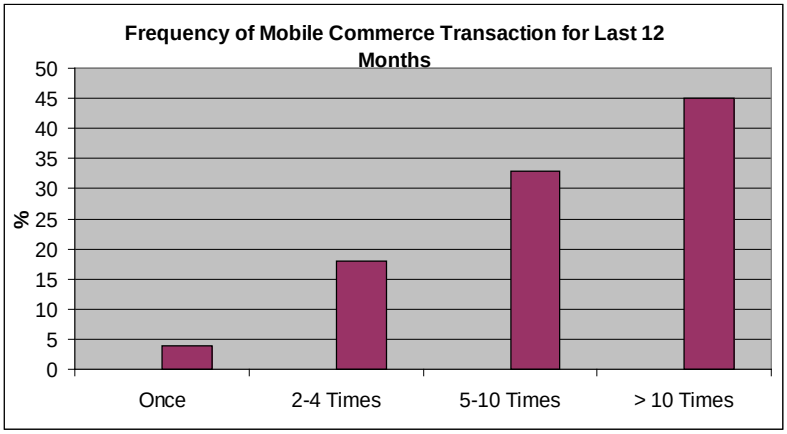


Figure 9. Types of m-commerce transactions done by Respondents for last 12 months.

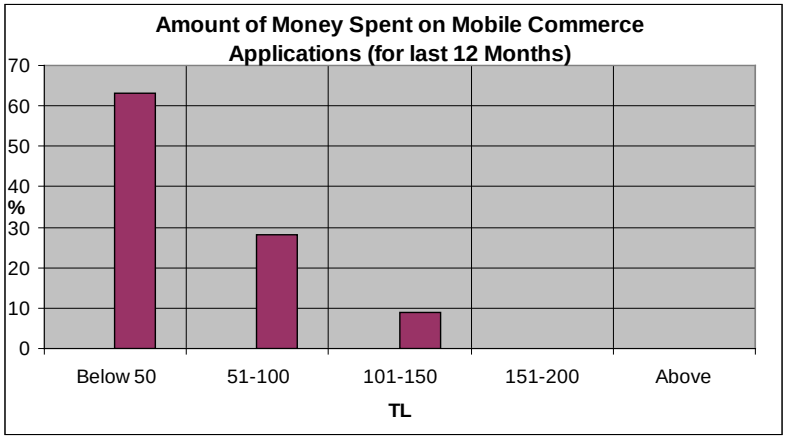


Figure 10. Amount of money spent on mobile commerce applications for last 12 months.

Table 10. Amount of money spent on mobile commerce applications for last 12 months.

Amount of Money (TL)	Number of Respondents	% of Respondents
Below 50	63	63%
51 - 100	28	28%
101 - 150	9	9%
151 - 200	0	0%
More Than 200	0	0%
Total	100	100%

Inference: According to the information gathered from the questionnaire analysis, it can be said that, a minority of respondents spend considerable amount of money on mobile commerce applications and majority of respondents spend less then 50TL on Mobile commerce applications.

4.10. Agreement Level of Respondents

Table 11 is showing the agreement levels of respondents against different statements. According to these statements only.

Inference: Table shows us the agreement level of some causes and it is found out that only first 4 ranks, 1st 2nd 3rd 4th rankings was highly agreed. According to this situation, it can be said that, due to occupation, marital status, because the popularity of technology and people characteristics effect the usage of mobile commerce.

4.11. Recommendation of Mobile Commerce Transactions by Respondents

Table 11 is showing the respondents recommendation of Mobile Commerce transactions to their relatives and friends. According to the gathered and analyzed data, %75 of respondents (75 respondent) answered as definitely recommend, %12 of respondents (12 respondent) answered as somewhat recommend, %10 of respondents (10 respondent) answered as No Comment, and 3% of respondents (3 respondent) answered as do not recommend the mobile commerce transactions for their friends and relatives.

Table 11. Agreement level of respondents.

S. No	Statements	Score	S. Score	Rank	Agreement Level
1.	I use mobile commerce transactions because I am single	242	12.1	17	Disagree
2.	I use mobile commerce transactions because I am married	364	18.2	4	Highly Agree
3.	I use mobile commerce transactions because I have children	269	13.5	16	Disagree
4.	I use mobile commerce transactions because I am educated	277	13.9	13	Disagree
5.	I use mobile commerce transactions due to my occupation	370	18.5	3	Highly Agree
6.	I use mobile commerce transactions because I have high income	236	11.8	18	Disagree
7.	I use mobile commerce transactions because I like to live a good life style	226	11.3	19	Disagree
8.	I use mobile commerce transactions because I want to show myself different from my friends	325	16.3	10	Agree
9.	I use mobile commerce transactions because I want show myself modern to my friends	274	13.7	14	Agree
10.	I use mobile commerce transactions because everyone in my society uses the same	341	17.05	7	Agree
11.	I use mobile commerce transactions because I want to get appreciation from society	329	16.5	8	Agree
12.	I use mobile commerce transactions because I want the society to respect me	273	13.7	15	Agree
13.	I use mobile commerce transactions because it is suitable to my culture	284	14.2	11	Agree
14.	I use mobile commerce transactions because it is useful for my work culture	341	17.1	6	Agree
15.	I use mobile commerce transactions because it helps me to align with my culture	282	14.1	12	Agree
16.	I use mobile commerce transactions because the technology save my time and money	356	17.8	5	Agree
17.	I use mobile commerce transactions to show I am a tech savvy (lover of technology)	373	18.7	2	Highly Agree
18.	I use mobile commerce transactions because it is the latest technology on commerce	387	19.4	1	Highly Agree

Table 12. Recommendation of mobile commerce transactions by respondents.

Opinion	Number of Respondents	% of Respondents
Definitely Recommend	75	75%
Somewhat Recommend	12	12%
No comments	10	10%
Do not Recommend	3	3%
Not at all	0	0%
Total	100	100%

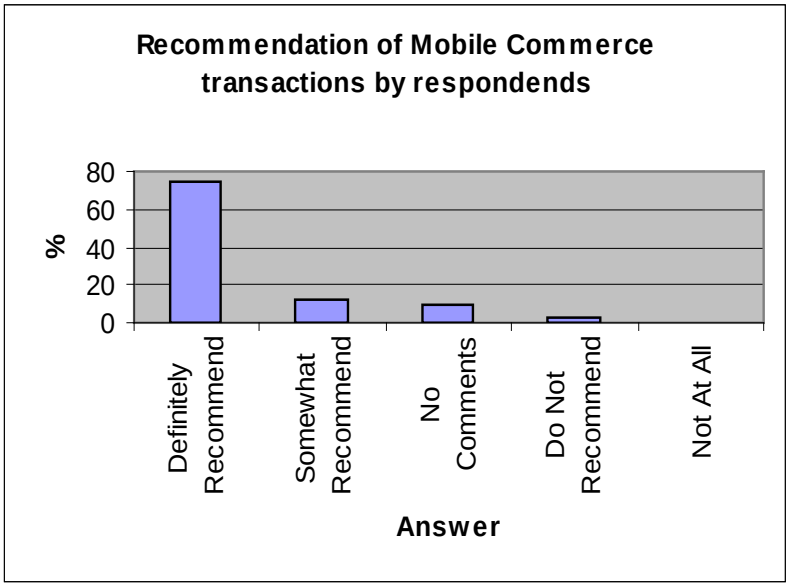


Figure 11. Recommendation of Mobile Commerce transactions by respondents.

Inference: According to the data in **Table 12** and **Figure 11**, it can be said that majority of respondents definitely recommend mobile commerce transactions, and very small minority of respondents do not recommend this technology. However, there are respondents exist in the middle who actually somewhat recommend or have no idea about this technology. It must be important to consider that portion of the sample.

5. Hypothesis Testing

At the Hypothesis formulation section of this study, the following hypothesis have been formulated which are;

H1: There is a significant impact of internal variables (demographic and psychographic variables) on consumer behaviour towards mobile commerce

H2: There is a significant impact of external variables (social, cultural and technology variables) on consumer behaviour towards mobile commerce.

According to the answers we gathered from the respondents and analyzing of these data, results are showing us that, H1 and H2 are correct. Because demographic and psychographic variables affecting the respondents behaviour towards mobile commerce in this study. **Table 11** showing the rankings of the ideas which gathered from the questionnaires of respondents. According to that information, usage of mobile commerce applications affected due to occupation, marital status, and because of the popularity of this technology in market and as well as people characteristics effect the usage of mobile commerce. This is showing that, both internal and external variables have a significant impact on mobile commerce.

6. Conclusions & Recommendations

This study was conducted on a small region of the country, but it can be a sample to analyse the consumer behaviour towards mobile commerce to provide better services or improve existence services in the regions. The findings can show us that, respondents are technology savvy and like technological improvements and developments. Some limitations may exist as mentioned above, and additionally, the competition between the mobile service providers can be one of the handicaps for mobile commerce services.

As it is stated at the end of the findings section, the outcome of the study can show us that people do not spend too much money on the mobile commerce transactions. However, Section 4.6 indicated that, the interactive services, such as chatting, games, etc. are most popular mobile commerce services used by the respondents.

Especially, some of the respondents stated that, the facebook and twitter web sites are the most visited and important websites for them. In this case, it is important to highlight those free access services launched by the mobile service providers in this region such as facebook, twitter and messenger and this must be considered as one of the reasons of low amount of money spent on mobile commerce transactions an outcome. On the other hand, because of the lack of mobile commerce infrastructure from the security point of view in the region, most of the m-commerce consumers couldn't highly satisfy. The study can be conducted by considering what type of services of mobile commerce is used by consumers, and under what circumstances consumer will rely on these services. Because some of the consumers, especially in such a region which infrastructure is not completely secure, the m-commerce cannot go further than a simple chatting tool and it cannot be used as a transaction tool for businesses as well as consumers.

Since this study has conducted at Cyprus Research Centre, it has limitations because of limited resources, time and population. It must be stated that, the research outcomes may vary if it conducts on different regions of the country with different populations.

Research outcomes may rely on the respondent's profile, or different characteristics of the respondents. This specific research is conducted mainly with the university student's participation. The student's perception against mobile commerce technology and monetary income may affect the outcomes of the study.

Mobile commerce applications can become more popular by providing more services, and customer feedback. People ideas and behaviour can indicate us that, they use this technology and they are lover of this technology, for that reason they are using this technology.

References

[1] Sari, A. (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. *International Journal of Learning and Development*, **2**, 18-30. http://dx.doi.org/10.5296/ijld.v2i2.1371

[2] Cellatoğlu, N. and Sari, A. (2010) Environmental Impacts of Private Transportation on Sustainable Development: A Case Study of Northern Cyprus. 1*st International Sustainable Building Symposium*, Volume 1, 441-445.

[3] Sari, A., Karaduman, A. and Firat, A. (2015) Deployment Challenges of Offshore Renewable Energy Systems for Sustainability in Developing Countries. *Journal of Geographic Information System*, **7**, 465-477. http://dx.doi.org/10.4236/jgis.2015.75037

[4] Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. *Global Journal of Sociology*, **4**, 41-45.

[5] Sari, A. (2012) Diversification of Tourism Activities in Small Island Developing States. *International Journal of Applied Science and Technology*, **2**.

[6] Yankee Group Research, Mobile User Survey Results Part 1: Will Next Generation Data Services Close the Value Gap? 2002.

[7] Instat/MDR. Worldwide Wireless Data/Internet Market: Bright Spots in a Dark Industry. 2002.

[8] Ghosh, A.K. and Swaminatha, T.M. (2001) Software Security and Privacy Risks in Mobile *e-Commerce. Communications of the ACM*, **44**, 51-57. http://dx.doi.org/10.1145/359205.359227

[9] Tarasewich, P. (2003) Designing Mobile Commerce Applications. *Communications of the ACM*, **46**, 57-60. http://dx.doi.org/10.1145/953460.953489

[10] Will, G. (2004) Upstart Airline Shows Direction of Industry. *The Chicago Sun-Times*, Chicago Sun Times Inc., Chicago. http://web.lexis-nexis.com

[11] Tsalgatidou, A., Veijalainen, J. and Pitoura, E. (2000) Challenges in Mobile Electronic Commerce. *Proceedings of IEC*

of the Third International Conference on Innovation through E-Commerce, Manchester, 14-16.

[12] Turban, E. (2004) Electronic Commerce: A Managerial Prospective. Pearson Education, Inc., Upper Saddle River.

[13] Boon, S. and Holmes, J. (1991) The Dynamics of Interpersonal Trust: Resolving Uncertainity in the Face of Risk. In: Hinde, R. and Gorebel, J., Eds., *Cooperation and Prosocial Behaviour*, Cambridge University Press, Cambridge, 190-211.

[14] Ambrose, P. and Johnson, G. (2000) A Trust Based Model of Buying Behavior in Electronic Retailing. *Proceedings of America Conference of Information System*.

[15] Hoffman, D., Novak, T. and Peralta, M. (1999) Building Customer Trust Online. *Communications of ACM*, **42**, 54-57. http://dx.doi.org/10.1145/299157.299175

[16] Ratnasingham, P. and Kumar, K. (2000) Trading Partner Trust in Electronic Commerce Participation. *Proceedings of International Conference of Information Systems*.

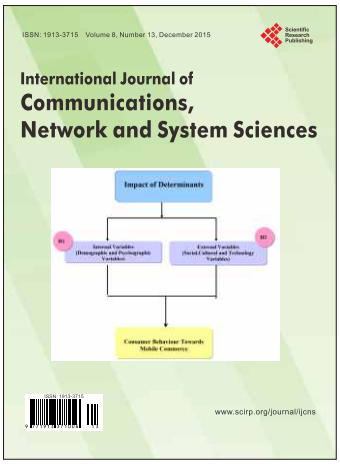
[17] Cheung, C. and Lee, M. (2000) Trust in Internet shopping: A Proposed Model and Measurement Instrument. *Proceedings of America Conference of Information System*.

[18] Androulidakis, N. and Androulidakis, I. (2005) Perspectives of Mobile Advertising in Greek Market. *Proceedings of* 2005 *International Conference on Mobile Business* (*ICBM* 2005). http://dx.doi.org/10.1109/icmb.2005.78

[19] Thornhill, A., *et al*. (2003) Research Methods for Business Students. 3rd Edition, Rotolito Lombarda, Italy, 72, 85.

[20] Robson, C. (1993) Real World Research. A Resource for Social Scientists and Practitioner Researchers. Blackwell Publishers Inc., Oxford.

Call for Papers



International Journal of Communications, Network and System Sciences (IJCNS)

ISSN 1913-3715 (Print) ISSN 1913-3723 (Online)
http://www.scirp.org/journal/ijcns

IJCNS is an international refereed journal dedicated to the latest advancement of communications and network technologies. The goal of this journal is to keep a record of the state-of-the-art research and promote the research work in these fast moving areas.

Editor-in-Chief

Subject Coverage

This journal invites original research and review papers that address the following issues in wireless communications and networks. Topics of interest include, but are not limited to:

Ad Hoc and Mesh Networks	Network Protocol, QoS and Congestion Control
Coding, Detection and Modulation	Network Survivability
Cognitive Radio	Next Generation Network Architectures
Communication Networks Architecture Design	Reconfigurable Networks
Communication Reliability and Privacy	Resource Management
Communication Security and Information Assurance	Satellite Communication
Cooperative Communications	Sensor Networks
Embedded Distributed Systems	Simulation and Optimization Tools
Global Networks	UWB Technologies
Heterogeneous Networking	Wave Propagation and Antenna Design
Microprocessor	Wireless Personal Communications
MIMO and OFDM Technologies	

We are also interested in short papers (letters) that clearly address a specific problem, and short survey or position papers that sketch the results or problems on a specific topic. Authors of selected short papers would be invited to write a regular paper on the same topic for future issues of the IJCNS.

Notes for Intending Authors

Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. Paper submission will be handled electronically through the website. All papers are refereed through a peer review process. For more details about the submissions, please access the website.

Website and E-Mail

http://www.scirp.org/journal/ijcns **E-Mail: ijcns@scirp.org**

What is SCIRP?

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

What is Open Access?

All original research papers published by SCIRP are made freely and permanently accessible online immediately upon publication. To be able to provide open access journals, SCIRP defrays operation costs from authors and subscription charges only for its printed version. Open access publishing allows an immediate, worldwide, barrier-free, open access to the full text of research papers, which is in the best interests of the scientific community.

- High visibility for maximum global exposure with open access publishing model
- Rigorous peer review of research papers
- Prompt faster publication with less cost
- Guaranteed targeted, multidisciplinary audience

Scientific Research Publishing

Website: http://www.scirp.org

Subscription: sub@scirp.org

Advertisement: service@scirp.org