Modern Applied Science; Vol. 12, No. 5; 2018
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Policy Based Approach for Information Transfer over Mobile ad hoc Network Using Messages Privacy Control

Faten Hamad[1] & Omar Adwan[2]

[1] School of Educational Sciences, The University of Jordan, Amman, Jordan

[2] King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

Correspondence: Faten Hamad, School of Educational Sciences, The University of Jordan, Amman, Jordan. E-mail: f.hamad@ju.edu.jo

Received: October 16, 2017 Accepted: February 28, 2018 Online Published: April 20, 2018

doi:10.5539/mas.v12n5p22 URL: https://doi.org/10.5539/mas.v12n5p22

Abstract

Ad Hoc networks are a set of wireless mobile communication nodes (stations, users) that exchange information between different nodes in a dynamic environment. The mobile infrastructure helps to form the dynamic network structure. Nodes communicate and send information between each other and with the centralized access points without interference. Each node acts both as a router to information or as an end user node that receives the sent information. Information dissemination between different nodes may face a lack of security due to accidental or unauthorized messages forwarded to an illegal third party. This paper proposes a policy based approach for information transfer over Mobile ad hoc network (MANET) using the messages privacy control, where the creator of the message determines the nodes that should receive the message and deny sending the message to other nodes. Each message is sent in combination with a policy which controls its sending behaviour at the receiver side. The policy is applied at the application level. A simulation of the proposed approach has been programmed to perform experimental case studies. The results have proven the efficiency of the proposed approach in securing the privacy of information transfer.

Keywords: information privacy, MANET, information dissemination, message security

1. Introduction

Mobile peer-to-peer networks are peer-to-peer, self-configuring networks based on router nodes that are interconnected by wireless communication channels and differ in that the topology of such networks varies. Each device in such a network moves independently of the others in absolutely any direction. Self-configurability is necessary in order for the connectivity of the nodes to be possible. Nodes, while functioning on the network, use a common wireless channel, and access to it is provided randomly (Bhattacharyya et al, 2018) (Chen and Liao, 2010). The nodes implement the transfer of information through retransmission. Therefore, the nodes in the network are not only hosts, but also routers for information transfer (Chen et. al., 2008). The most important features of such networks are; the existence of a peer-to-peer structure and decentralized management; the presence of an unpredictably and dynamically changing topology; availability of the routing function for all nodes; self-organization of the network (through retransmission); various limiting factors in the network in the form of range of radio visibility or capacity of battery devices; and finally, large information loss (Chen, et. al., 2011)) (Bychkovsky et al., 2006) (Chaudhry et al., 2018). Wireless communication networks are divided into centralized infrastructures and self-organizing ones. A distinctive feature of self-organizing networks (SON) is the ability, in the absence of a centralized infrastructure, to exchange information for any pair in the radio coverage area of network nodes. Nodes in SON can be both end hosts and routers. The connection is organized over long distances with the help of specialized routing protocols in intermediate router nodes (Bose et al,. 2007);(Briesemeisterand Hommel, 2000). This connection is called "multi-stage or multi-step" (multi-hop). The stage is the participation of one router node in this connection. The nodes of these networks, which can find each other and form a network, and in the event of the failure of any node, they can impose new routes for sending messages (Luo et al., 2006); (Kibria el al., 2008).

1.1 Self-Organized Networks

Ad Hoc wireless mobile network (MANET); Wireless Sensor Networks (WSN); Wireless Mesh Network (WMN). Auto-vehicle wireless networks of the automobile network Ad Hoc (VANET).

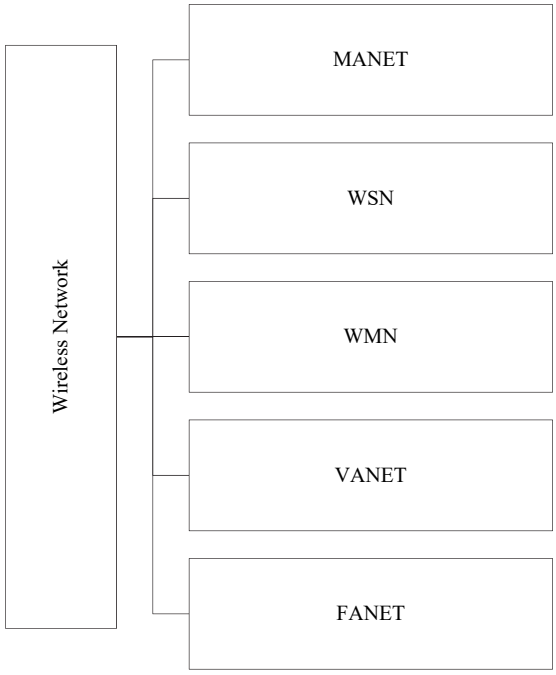

Figure 1. Wireless Network

1.2 MANET Network

In the MANET network, mobile devices do not only act as the functions of terminal stations, but also the functions of network nodes (routers). There are some areas of application of MANET networks, and the most widely used mobile networks are Ad Hoc for processing communications during combat operations. This establishes the connection between soldiers on the ground, in water and air transport (Maheshwari, Gour, & Chourasia, 2014); (Sandeep & Kumar, 2015). Most communication nodes move with different speeds. Networks with fixed infrastructure cannot provide reliable communication under such conditions of a high rate and a high degree of unpredictability (Srivastava & Kumar 2018). The system administrator has little time to react and reconfigure the network. As a rule, the MANET network does not require administration. A temporary Ad Hoc network can be deployed when infrastructure creation is impossible or inefficient. Such a network can be used as a temporary solution at conferences, as well as in unoccupied places where it is very difficult to create an infrastructure (Patel & Shah 2016)(Hudaib et al., 2016).

MANET technologies are used in industrial and commercial applications, including information exchange with mobile devices. In addition, mobile mesh networks can be an inexpensive fault-tolerant alternative to cellular networks (Hudaib and Fakhouri, 2016). There are military needs in fault-tolerant, compatible with IP services for mobile wireless communication networks (Maheshwari, Gour, & Chourasia, 2014). Many of which consist of very dynamic autonomous topological segments. Furthermore, the domain of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources to large-scale, mobile, highly dynamic networks. Significant examples include establishing survivable, efficient, dynamic communication for: network-centric military/battlefield environments, emergency/rescue operations, disaster relief operations, intelligent transportation systems, conferences, fault-tolerant mobile sensor grids, smart homes, patient monitoring, environment control, and other security sensitive applications. Most of these applications demand a specific security guarantees and reliable communication. (Hoebeke et al, 2004) (Sahingoz et al., 2012). Some well known applications are: Military Tactical Operations: For fast and possibly short term establishment of military communications and troop deployments in hostile and/or unknown environments, search and Rescue Operations: For communication in areas with little or no wireless infrastructure support, disaster Relief Operations: For communication in environments where the existing infrastructure is destroyed or left inoperable, law Enforcement: For secure and fast communication during law enforcement operations, and commercial Use: For enabling communications in exhibitions, conferences and large gatherings. For some business scenarios, the need for collaborative computing might be more important outside office environments than inside a building. (Hoebeke et al, 2004) (Goyal et al, 2011)

One of the problems of implementing class networks MANET is to ensure efficiency, security and reliability of information transmission in the conditions of arbitrarily changing physical network topology. This problem can be solved with a suitable implementation of security protocol (Anuradha & Mala, 2017). The key role in the decision is played at the protocol transport level. Protocols at the transport level guide the work from the above standing levels down to the application level. Therefore, reliable delivery protocols are needed for the operation of many network applications (Kumari, Kumar, & Bajaj, 2018).

1.3 Characteristics of MANET Networks

The MANET network consists of mobile platforms referred to as "nodes", which can be arbitrarily moved. Nodes can be placed on airplanes, ships, trucks and even people and every router can have many hosts. MANET is an autonomous system of mobile nodes. The system can work either isolated or have gateways or interfaces to fixed networks. In the latter case, such a network is usually considered as a stub network connected to a fixed network. End networks transmit traffic off their nodes. However, it does not allow the transmission of "transit" traffic (Khinchi & Bhushan, 2016); (Kumari, Kumar, & Bajaj, 2018).

The MANET nodes are equipped with wireless transmitters and receivers that use antennas that can be unidirectional for broadcast directed to point-to-point connections, possibly, manageable. Combinations of these antennas may also be used. At each moment, depending on the location of the nodes, coverage areas of their receivers and transmitters transmit power level and level interaction between the channels of the picture of the wireless connectivity that has the form of a random multi-hair (multihop) or an ad hoc network. The topology of such a network can change over time as a result of moving nodes or change their reception and transmission parameters (Johnson et al,. 2004); (Tamilarasan, 2012).

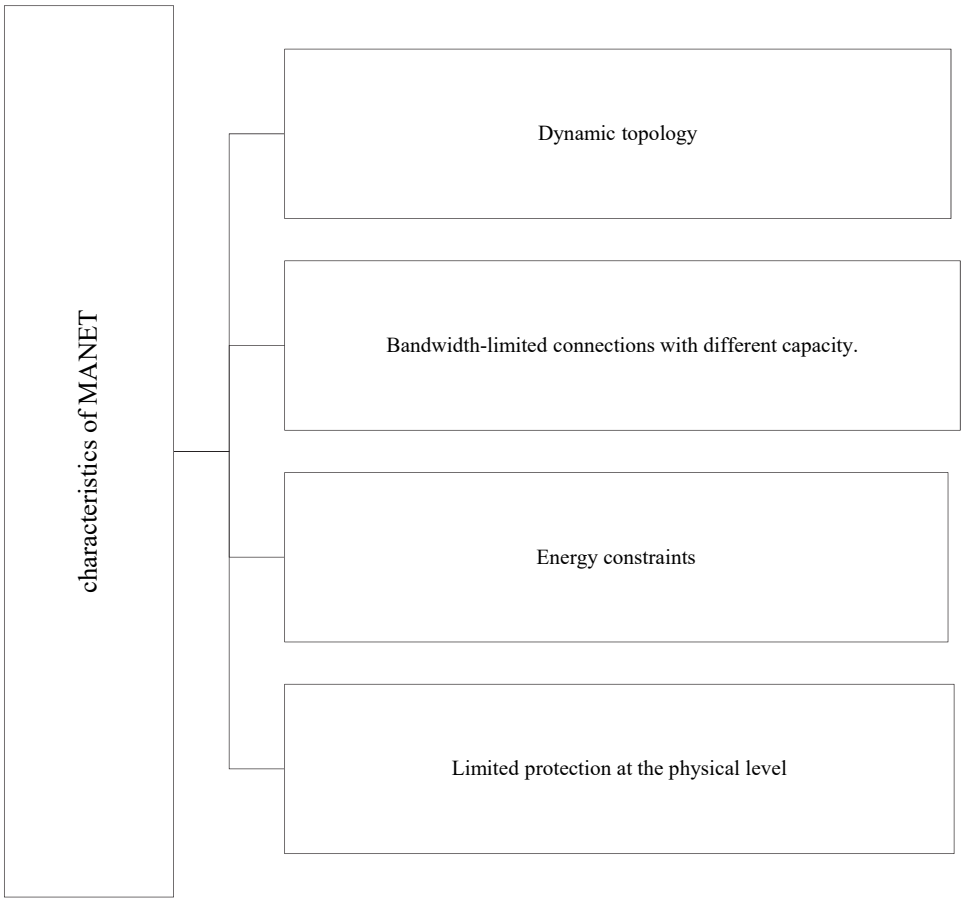

Figure 2. Characteristics of MANET

There are four distinguished characteristics for MANET (Chitkara, & Ahmad, 2014); (Kim, Min, & Kim 2004):

1) Dynamic topology: Network nodes can move arbitrarily and the network topology (usually includes multiple routing intervals) can quickly and randomly move into unpredictable moments, and can also include two-way and one-way connections.
2) Bandwidth-limited connections with different capacity: Wireless Connectivity substantially lost in the bandwidth of the cable lines. In addition, the throughput wireless connections, taking into account the effects of multiple access, attenuation, noise, interference and etc., is often significantly lower than the maximum speed in the radio channel. Relatively low bandwidth makes congestion in the network, a rule rather than Exceptions - the total application needs are often close or network capacity. Because mobile networks are often simply an extension of the existing infrastructure, users of these networks usually want to receive the same services as a fixed connection. User requests will grow as the number of applications grows multimedia and expanding collaboration through the network.
3) Energy constraints; Part or all of the MANET network nodes can run on batteries or other sources with limited capacity. Energy saving issues play an important role for such nodes.
4) Limited protection at the physical level: Mobile wireless networks are generally less protected from physical security threats, rather than cable networks. It is necessary to take into account a more high probability of interception and substitution of information, as well as attacks on the denial of services. Usually, wireless networks use different methods of protecting channels. For instance, a decentralized MANET's network management provides additional fault tolerance in comparison with centralized systems.

Despite the distinguish characteristics of MANET. It has weak points; not all nodes in MANET are equally trusted thus mistakenly message forwarding in any node may cause a serious harm. Worse yet, mobile nodes in tactical environments are subject to the danger of being captured or malfunction. Even a small number of misbehaving nodes can render the entire MANET inoperable: malicious peers can abuse the network exhausting all network and power resources. Messages transferred in MANET network has to reach its target receiver and not being forwarded after receiving it to other untrusted node especially in commercial or military usage (Zhao et al., 2007)(Namboodiri et al., 2004)

To address this problem policy based approach for information transfer (PAIT) has been proposed to control messages privacy data transfer over Mobile ad hoc network (MANET) where each message is combined with a policy before being sent to control its behaviour at the receiver side. However, the creator of the message determines the node or group of nodes that should receive the message and deny sending the message and he determine the classification of the message (Normal, Important, and very important).

The rest of the paper is organised as follows. Section two describes PAIT and its main components, pseudocode and main functionality. Section three describe the simulation and experimental evaluation including case studies, simulation and results analysis. Finally the conclusion is illustrated in section four.

2. Policy Approach for Information Transfer (PAIT)

This paper proposes a policy based approach by adding a policy to the sent messages that defines how the message will be used in the receiver side. The creator setup the confidentiality requirements of the message and determine the message's policy. PAIT specifies the disseminating security requirements of MANET messages. The transfer policy in PAIT is a set of rules which control how messages can be securely disseminated to other destinations without being disclosed to unwanted nodes in the network. PAIT policy is designed to protect the message confidentiality that is expressed by the creator.

Usually the message creator and sender have concerns about their confidentiality and privacy when the message is transferred from node to another. To solve the privacy concerns regarding the message security, the creator of the message can set and determine the policy that a node should possess regarding the sensitive MANET disseminated message.

In PAIT the structure of the transferred packet is improved by attaching a policy with each message. Two new policy based protocol agent packet structures were designed. The first packet that is sent is the sending packet, as shown in Figure 3. And the second is the Acknowledgement (Figure 4). The Acknowledgement consist of two parts; the first is the Acknowledgement of receiving the message itself and the second packet is the Acknowledgement of the policy after the decision component analyze it, see figure 5.

Sender address	Creator address	Destination address	The target address	Size	Acknowledgement flag	Packet order	Message	Policy

Figure 3. Sending packet structure

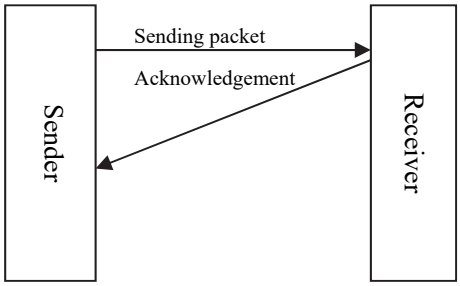

Figure 4. Message Acknowledgement

Message Acknowledgement	Policy Acknowledgement

Figure 5. Acknowledgement two parts

3.1 Information Transfer Policy

Policy is a deliberate system of principles to guide decisions and achieve rational outcomes (Williams et al., 2002). It is a set of ideas or plans that is used as a basis for making decisions, especially in politics, economics, or business (Collins dictionary, 2018). Policies that are used to assist in subjective decision making usually assist senior management with decisions that must be based on the relative merits of a number of factors, and as a result, are often hard to be tested objectively (Masa, and Parravicini, 2003).

In this paper, Policy refers to the set of rules that the message creator adds to the sent message to control the confidentiality of the message and how it should be transferred between nodes. It determines which node is allowed to send the message or deny it from sending. The Policy can be read and understood between all of the homogeneous components of PAIT. It is attached to the message, and will express the message creator confidentiality requirements to control the flow of messages between network nodes.

3.2 PAIT Policy Rule Consists of the Following Specifications

- *Message permission (permits (P) or denies (D))*
- *Classification of message: Normal (N), important (M), Very important (VIP)*
- *The targeted receiver or group of receiver nodes (GR)*

For instance, the rule: P VIP GR2, indicates that the message is classified as very important and is permitted to be sent to all nodes in the group with Id 2. PAIT Policy Rules is inspired by the Access Control List (ACL) language which is used in Unix Linux and Solaris operating systems. ACL contains a list of permissions attached to an object. Similarly, PAIT contains a list of permission rules that determine which nodes are allowed to access, send, deny, and receive the message.

The creator provides the message, message type (*Normal (N), important (M), Very important (VIP)* and the destination. The destination is formally expressed in the policy of the information transfer, this aims to enable PAIT to control the message flow between nodes of MANET.

PAIT provides a contribution by combining the transfer policy and the sent message in the packet structure. As illustrated in Figure 6, the communication model between the components describes how the message will be sent and received between the network nodes, starting from the creator node to the receiver node.

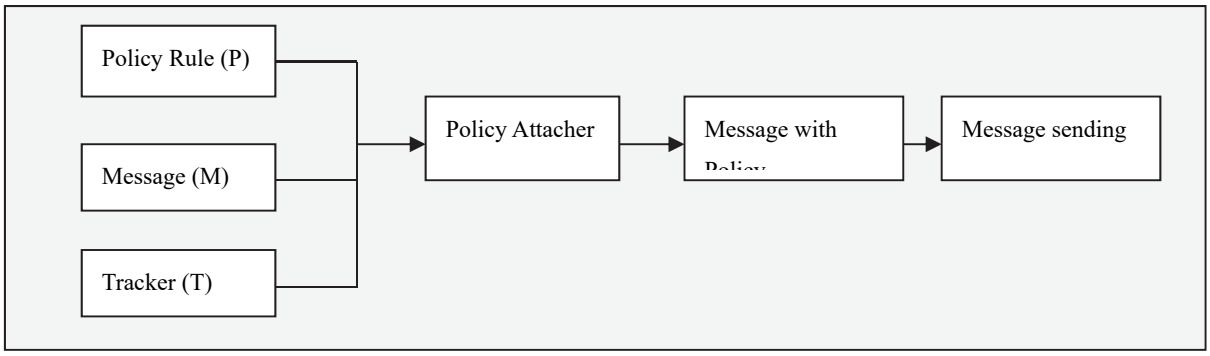

Figure 6. Sender side

PAIT functions at the application layer of the node, where every message will have a policy added to it. PAIT intercepts all of the arrived messages. The policy splitter component extracts the policy (P) and message (M) and tracker (T) from the received message. The Policy decider component will read the policy (P) then decides if the message should be forwarded or denied. It decides to which node or group of nodes the message should be forwarded and it also analyse the message classification (Normal, important, very important), Figure 7.

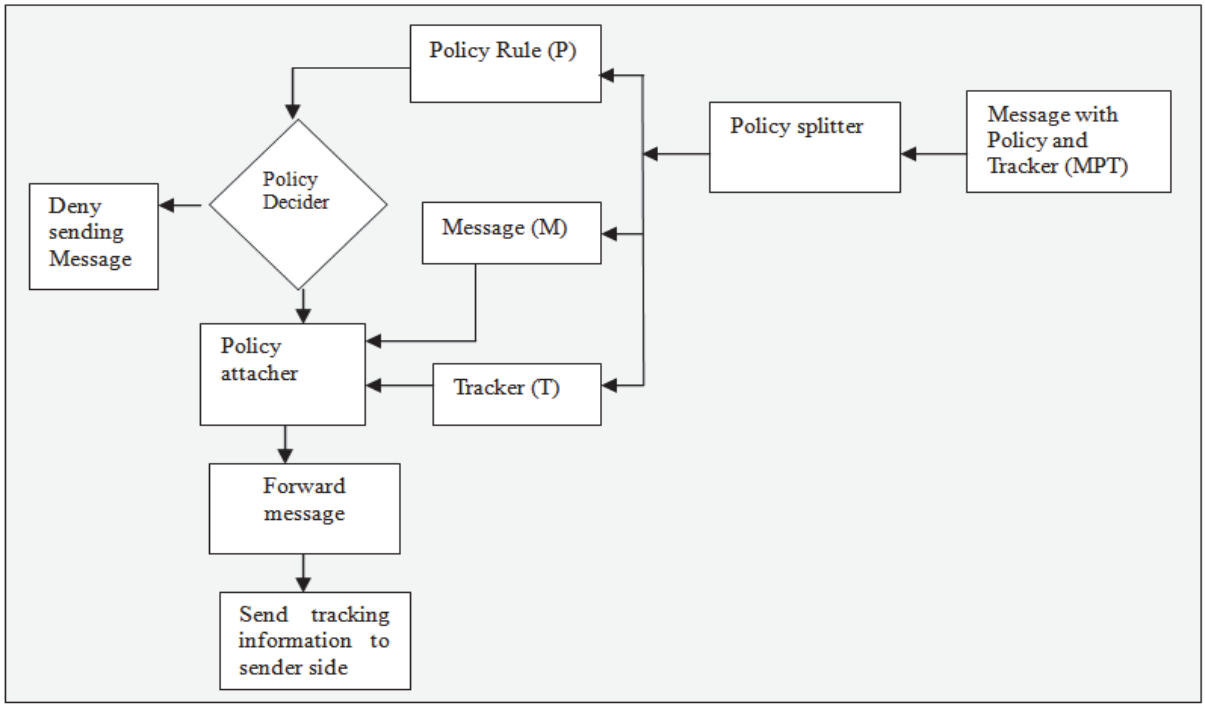

Figure 7. Receiver side

In case the decider component approves forwarding the message, the policy attacher component reattaches the policy and sends it to the specified nodes. Further the tracker component sends the tracking information to the message sender side. The pseudocode that illustrates the work of the decider component is illustrated in the Figure 8.

```
Read message M
Read transfer policy
Read old transfer policy for the message sender S
IF message first time received from sender
Send confirm transfer policy to sender
If confirmed
Read Classification C
Read Group G
Read Tracker T
Send Message to group G according to Classification C
Else
Deny sending the message M
Send notification to the Sender and Creator End if
IF message number of message received from sender > 1
Read sender transfer policy messages from archive
If transfer policy messages from archive = received policy
Apply transfer policy action to message M according to equation 2, 3
Else
Send confirm message M
If received confirmation policy to message M
Apply transfer policy action to message M according to equation 2, 3
Else
Ignore message
```

Figure 8. Pseudocode that illustrate the work of the decision component

Each message (M) that will be sent, has a policy attached to it that contain a Prevent deny (PD) value of 0 or 1, where 0 means denying the message from being sent and 1 approve the message to be sent. The group value specifies the group or node that the message will be sent to. The classification value specifies the message to be either *Normal (N), important (M), Very important (VIP)*. The tracker traces the flow of information contained in the message M.

If the receiver or any application on his device wants to forward the message then the sending decider component in PAIT will read the message and handle the request to send action. The Policy Decider determines to either deny sending the message or permit sending it. If any other application tries to send the message that was denied then PAIT sends a notification message to both the sender and the message creator.

3. Simulation and Experimental Evaluation

To test and evaluate PAIT performance a simulation has been performed using Cygwin environment for windows, and Ns2 simulator. Since most of the research in ad hoc networks use Network Simulator (NS-2) (Henderson et, al,. 2008), NS-2 was used to simulate the results. The experimental parameters for the simulation are listed in Table 1. The simulation of the results has been performed with different User Datagram Protocol (UDP) to check how the time necessary for a packet to be transmitted across a network from source to destination will be affected.

Table 1. Experimental Parameter

Number of nodes	0 ,10, 20, 30, 40, 50, 60, 70, 80
Network area	2000m * 2000m
Total simulation time	5000s
Speed	0 , 20, 40, 60, 80, 100, 120, 140, 160, 180, 200
Radio range	500 m
Network simulator	Ns2
Network area	2000m * 2000m

For The simulation a new packet structure and a new agent protocol suitable for NS-2 protocol was designed based on an existing class in NS-2. The Agents in class NS-2 that are used to implement protocols at different layers were also used. They are used as endpoints where packets are being assembled or consumed. The agent (policy) supports forwarding packets, receiving, sending, decryption, and encryption, check policy, write to policy file, and read from policy file. In order for the PAIT to work properly, we assume that it will and should be applied in every node of the communicated network at the application layer.

For the experimental results, two cases were tested: 1) the non-encrypted message and policy and 2) the encrypted message and policy using security function in NS-2 that add encryption and decryption algorithms functionality.

The evaluation aims at measuring the feasibility of the implementation average delay performance and evaluating the ability of message creator to control the aim of the approach and the proposed policy of information transfer between nodes using NS-2 simulator. For the evaluation, many experiments has been performed and the average delay has been calculated for both the messages sent with policy according to the proposed approach and messages without policy as shown in figure 12.

Two case studies have been explained, the first case study consists of 5 nodes and the second case study consists of four node as shown in figures 10 and 11 respectively. An assumption was made for the first case study as the following: there are 5 nodes, each has an id and belongs to 4 groups (gr1, gr2, gr3, and gr4), group gr1 contain node 1, group gr2 has node 2, 3, group gr3 has node 4, group gr4 has node 5, Figure 9.

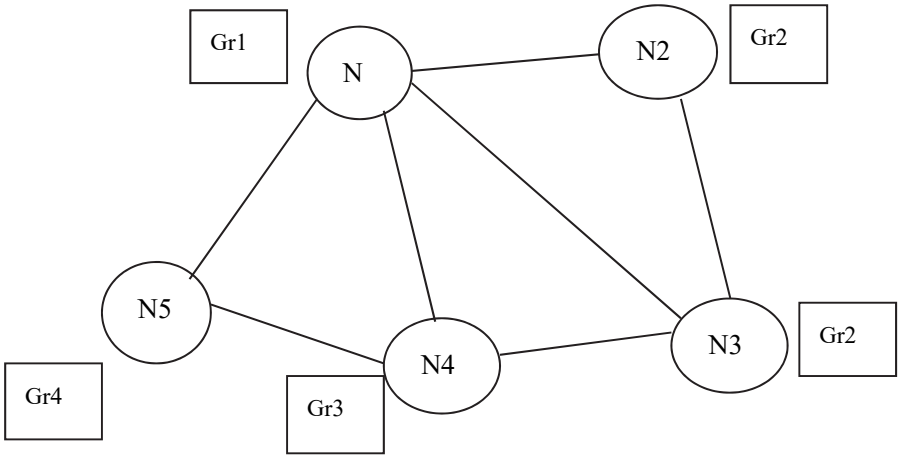

Figure 9. Five Node case study

Case study 1:

An assumption that node 1 want to send a message which is classified as very important one to node 3 was made, Our assumption policy: permit normal message to be sent to group1, 2 and 3, permit very important message to be sent to group 2, deny very important message to be sent to group 3, permit important message to be sent to group 3, deny important message to be sent to group 2. These conditions are specified in the policy file at node0.txt in node 0. These conditions will be called information transfer policy rules.

Node 1 policy rules are:

1- P N GR1
2- P N GR2
3- P N GR3
4- P N GR4
5- P VIP GR2
6- D VIP GR3
7- P VIP GR4
8- P IM GR2
9- P IM GR3
10- P IM GR4

When node 2 or 3 receive a very important message from node 1 and its' destination is node 5, it will check its policy before sending the message to the destination node; if the policy permits then it will send the message with the policy of node 1 regarding the sent message to node 5. Then node 5 will receive the message and send an acknowledgment message to node 2 which send an acknowledgment message as well to node 1. But if node 2 want to send the message to node 4 which is in group 3 (are set to be denied to receive VIP message) then it check the policy which illustrate the deny policy for group3, node 4, and so node 2 will note send the message to node 4.

The discussion and results of previous case study showed that the implemented policy approach succeed in either deny or permit the sending of messages according to the creator rules, and the creator node was able to control the flow of messages between all nodes in the network. The NS-2 simulator provided a good illustration of the real network and applying the policy approach. The results of applying the policy to the process of sending the message and the acknowledgment have followed the creator node rules. The policy has been attached to the message and transferred from node to other node in the network.

The assumption for the second case study; is that there are 4 nodes, each has an id and belong to 4 groups (gr1, gr2, gr3, and gr4), group gr1 contain node 0, group gr2 has node 1, group gr3 has node 2, group gr4 has node 3, Figure 10. Figure 10(a, b and c) show that the 4 nodes are connected together where node 0, 1 are connected to node 2 and node 2 is connected to node 3, each node has its policy according to the group that it belongs to. In this case study an assumption that both node 0, 1 send packets to node 3 through node 2 was made, as shown in Figure 10 (a, b and c), each one of node 0, 1 and node 3 has a separate group policy for sending and receiving. For instance, when node 2 receives a packet from node 0, first it checks its policy then decides where to forward the packet. Accordingly, to node 2 will forward the packet to node 3 only but not node 1. As illustrated in Figure 10 (b) when node 3 receives the packets it sends back an acknowledgment to node 0 to acknowledge the receiving of the packets, the acknowledgment will be transferred to node 0 through node 2 as shown in Figure 10 (d, e and f). All of the nodes in this case study have the policy framework in the application level.

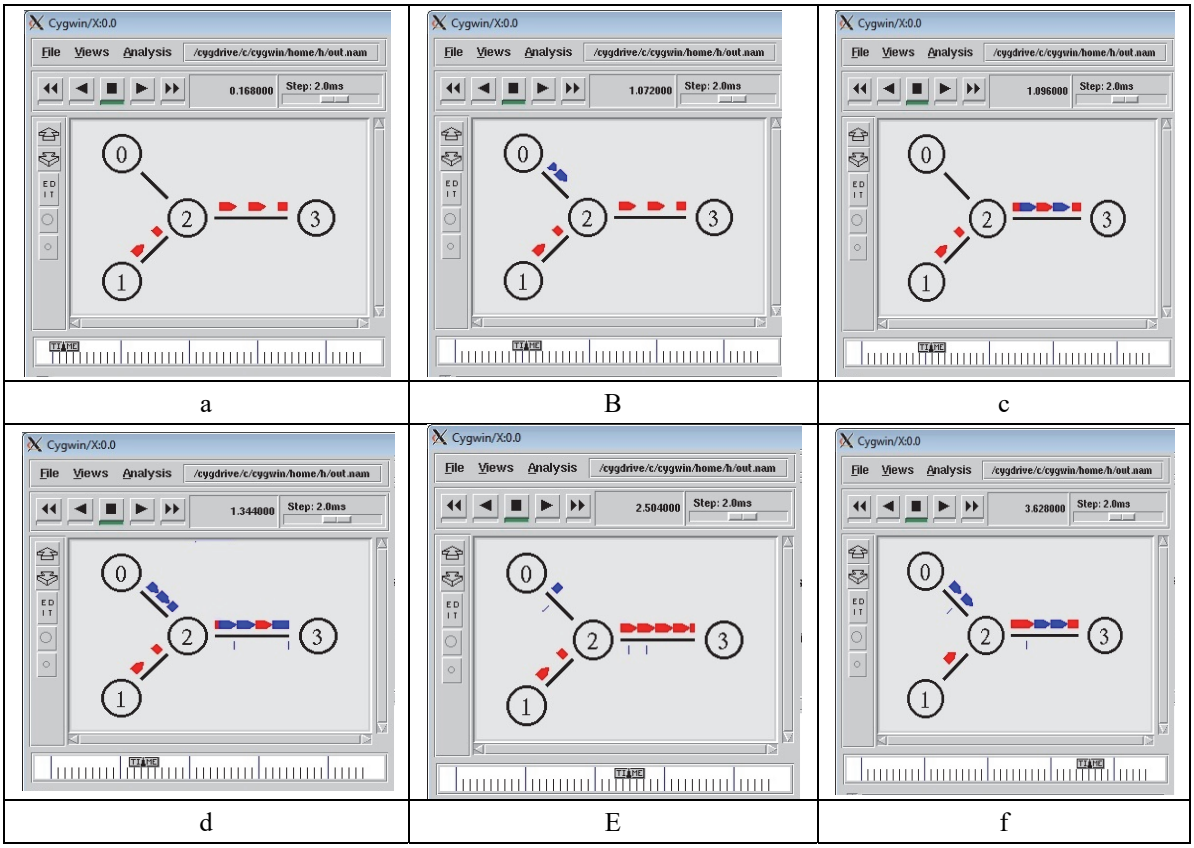

Figure 10. Simulation of first case study with Four nodes

Next, the delay time versus number of messages sent (traffic) was measured, which are depicted on the y-axis and x-axis respectively. The results indicated that as the number of the sent messages increases, the delay time of both type of messages (with and without policy) increases, however, it can be noticed that the delay time for the massages with the policy is slightly higher than the one without policy. However, although that the proposed approach have a higher delay time than the methods to send messages without policy; still, the delay time is un-noticeable as it ranges between 0.0001 to 0.0007 milliseconds and therefore it will not affect the performance of message sending with policy as shown in figure 11.

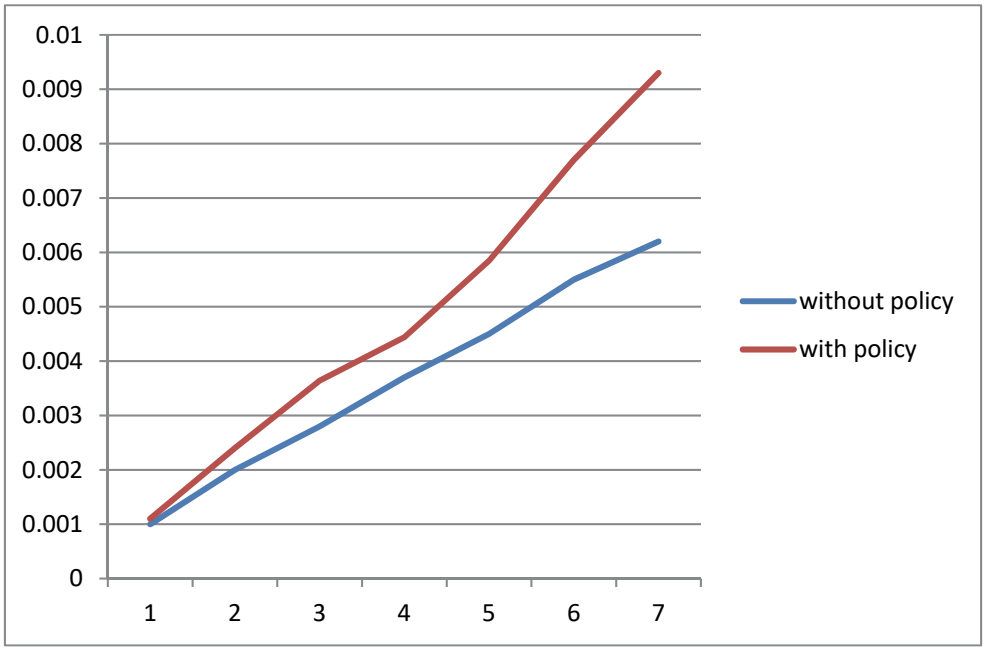

Figure 11. Delay of sending packets for both the proposed approach (with policy approach) and without policy

6. Conclusion

In this research an approach that illustrates how to control the information transfer and confidentiality between nodes was developed. The approach suggested using a policy rules that is attached to the message and these rules will be read and analyzed by the received nodes at the application level. It has been experimentally tested using NS-2 simulator and a new packet structure has been suggested to fit the new policy assumption. The experimental tested cases results of the studies have proven the efficiency of the policy based approach to control information dissemination in MANET using messages privacy control.

References

Anuradha, M., & Mala, G. A. (2017). Cross-layer based congestion detection and routing protocol using fuzzy logic for MANET. *Wireless Networks*, *23*(5), 1373-1385.

Hudaib, A. A., Fakhouri, H. N., Al Adwan, F. E., & Fakhouri, S. N. (2016). A Survey about Self-Healing Systems (Desktop and Web Application). *Communications and Network, 9*(01), 71.

Bhattacharyya, D., Chatterjee, A., Chatterjee, B., Saha, A. K., & Santra, A. (2018). A novel approach to energy efficient low cost routing in MANET by reduction in packet size. In Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual (pp. 679-684). IEEE.

Bose, S., Bharathimurugan, S., Kannan, A. (2007). Multilayer Integrated Anomaly Intrusion Detection System for Mobile Ad Hoc Networks, IEEE ICSCN 2007, MIT Campus, Anna University, Chennai, India, pp.360-365.

Briesemeister, L., & Hommel, G. (2000). Role-based multicast in highly mobile but sparsely connected ad hoc networks. In *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on* (pp. 45-50). IEEE.

Bychkovsky, V., Hull, B., Miu, A., Balakrishnan, H., & Madden, S. (2006, September). A measurement study of vehicular internet access using in situ Wi-Fi networks. In *Proceedings of the 12th annual international conference on Mobile computing and networking* (pp. 50-61). ACM.

Chaudhry, R., & Tapaswi, S. (2018). Optimized power control and efficient energy conservation for topology management of MANET with an adaptive Gabriel graph. *Computers & Electrical Engineering*.

Chen, J. B., & Liao, S. J. (2010). A fuzzy-based decision approach for supporting multimedia content request routing in cdn. In *Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on* (pp. 46-51). IEEE.

Chen, W., Guha, R. K., Kwon, T. J., Lee, J., & Hsu, Y. Y. (2011). A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, *11*(7), 787-795.

Chitkara, M., & Ahmad, M. W. (2014). Review on manet: characteristics, challenges, imperatives and routing protocols. *International Journal of Computer Science and Mobile Computing, 3*(2), 432-437.

Collins Dictionary. (2018). Retrieved January 2, 2018, from: https://www.collinsdictionary.com/dictionary/english/policy

Henderson, T. R., Lacage, M., Riley, G. F., Dowell, C., & Kopena, J. (2008). Network simulations with the ns-3 simulator. *SIGCOMM demonstration, 14*(14), 527.

Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., & Viennot, L. (2001). Optimized link state routing protocol for ad hoc networks. In *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International* (pp. 62-68). IEEE.

Johnson, D. B., Maltz, D. A., & Hu, Y. C. (2004), The Dynamic Source Routing protocol for mobile ad hoc networks", Internet Draft.

Khinchi, M. K., & Bhushan, B. (2016). Secure Synchronous MANET Routing Policy to Achieve High Performance and Efficiency in Wireless Network.

Kumari, N., Kumar, R., & Bajaj, R. (2018). Energy Efficient Communication Using Reconfigurable Directional Antenna in MANET. *Procedia Computer Science, 125,* 194-200.

Li, S. Y. R., Sun, Q. T., & Shao, Z. (2011). Linear network coding: Theory and algorithms. *Proceedings of the IEEE*, *99*(3), 372-387.

Luo, Y., Wang, J., & Chen, J. (2006). Algorithm based on mobility prediction and probability for energy efficient multicasting in ad-hoc networks. *Computer Research and Development, 43*(2), 231-237.

Kibria Ma, Y., M. R., & Jamalipour, A. (2008, November). Cache-based content delivery in opportunistic mobile ad hoc networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (pp. 1-5). IEEE.

Maheshwari, G., Gour, M., & Chourasia, U. K. (2014). A survey on congestion control in MANET. *International Journal of Computer Science and Information Technologies (IJCSIT), 5*(2), 998-1001.

Masa, M., & Parravicini, E. (2003, April). Impact of request routing algorithms on the delivery performance of content delivery networks. In *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International* (pp. 5-12). IEEE.

Mukhtar, R., & Rosberg, Z. (2003, April). A client side measurement scheme for request routing in virtual open content delivery networks. In Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International (pp. 233-240). IEEE.

Namboodiri, V., Agarwal, M., & Gao, L. (2004, October). A study on the feasibility of mobile gateways for vehicular ad-hoc networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks* (pp. 66-75). ACM.

Naumov V., Baumann R. and Gross T., (2005), The Study of Inter-Vehicle Ad Hoc Networks on Realistic Vehicular Traces, In MobiHoc '06: proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing, pp. 108-119.

Pals, H., Petri, S., & Grewe, C. (2000, May). FANTOMAS fault tolerance for mobile agents in clusters. In *International Parallel and Distributed Processing Symposium* (pp. 1236-1247). Springer, Berlin, Heidelberg.

Papadopouli, M., & Schulzrinne, H. (2001, October). Effects of power conservation, wireless coverage and cooperation on data dissemination among mobile devices. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing* (pp. 117-127). ACM.

Patel, K. S., & Shah, J. S. (2016). Study the Effect of Packet Drop Attack in AODV Routing and MANET and Detection of Such Node in MANET. In Proceedings of International Conference on ICT for Sustainable Development (pp. 135-142). Springer, Singapore.

Ros, F. J., Ruiz, P. M., & Stojmenovic, I. (2012). Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks. *IEEE Transactions on Mobile Computing*, *11*(1),

33-46.

Sahingoz, O. K., & Sonmez, A. C. (2012). Agent-based fault tolerant distributed event system. *Computing and Informatics*, *26*(5), 489-506.

Sandeep, J., & Kumar, J. S. (2015). Efficient packet transmission and energy optimization in military operation scenarios of MANET. *Procedia Computer Science*, *47,* 400-407.

Srivastava, P., & Kumar, R. (2018). A Timestamp-Based Adaptive Gateway Discovery Algorithm for Ubiquitous Internet Access in MANET. In Next-Generation Networks (pp. 153-162). Springer, Singapore.

Tamilarasan, S. (2012). A quantitative study and comparison of AODV, OLSR and TORA routing protocols in MANET. *International Journal of Computer Science Issues(IJCSI), 9*(1).

Williams, B., & Camp, T. (2002). Comparison of broadcasting techniques for mobile ad hoc networks. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* (pp. 194-205). ACM.

Zhao, J., Zhang, Y., & Cao, G. (2007). Data pouring and buffering on the road: A new data dissemination paradigm for vehicular ad hoc networks. *IEEE transactions on vehicular technology*, *56*(6), 3266-3277.