Trust based Security Management in Wireless Adhoc Network : A Review

Amrit Singh[1], Dr. Anoop Sharma[2], Dr. Ajay Goyal[3]
[1]*School of Computer Science and IT, Singhania University*
[2] *School of Computer Science and IT, Singhania University*
[3] *Faculty of computational science, GNAUniversity Phagwara*
E-mail: prof.as.madahar@gmail.com

***Abstract*—** Ad Hoc Network is a decentralized wireless network that does not require the pre-existing infrastructure. In this each of the note participate in the routing by sending the data to the other consecutive node. As the Ad Hoc Networks network is a wireless based networks, it faces different security challenges that makes the network vulnerable. This gives the challenge to identify the trusted nodes for which trust based modeling for assessment the node and the routing process. In this paper different literature were discussed that focus on applying different security techniques such as OLSR, Fuzzy logics, MANETs etc. That mainly concentrates on the best route selection method, and next trusted node selection after applying these security techniques.

Keywords*—Ad Hoc Network communication, Secure Routing.*

I. INTRODUCTION

Ad Hoc Networks are the wireless based networks that has the self-organizing properties. It does not check for any infra based on physical attribute in order to be absorbed in the required environment. Hubs and Nodes for this especially appointed system of Ad Hoc Networks shows the properties of both the router and the client. Some of the applications of these appointed systems are in the field of mechanical and business industries with the possibilities of adaptable exchange of information [1]. The previously developed systems such as remote sensor systems (WSNs), Internet of Things (IOT), wearable computing and pervasive processing have added the possibilities for the future advancements of the specially appointed systems [2]. The Ad Hoc Networks are known as totally self-dependent remote brief system for emergency and crisis situations as well as for military where other frameworks were not accessible [3].

1.1 SECURITY ISSUESS IN AD HOC NETWORKS

These are some of the security challenges that were generally faced in the Ad Hoc Networks.

- The networks based on wireless technique are exposed for the link attacks such as passive and active link attack like eavesdropping and active interfering respectively. Whereas in the wired networks, high amount of prevention is provided from the attacks by using the techniques like gateway and firewalls. But in the wireless system the all directions are open to be attacked and can be aimed at any of the node. Due to these vulnerabilities of wireless network confidential data are at risk. That leads to the violation of security rules. Hence it becomes important that each of the nodes present in the network have the capability to resist these kinds of attacks whether it would be a direct attack or an indirect attack.
- The individual nodes present in the network are vulnerable and can be easily attacked. These node can easily be attacked from both sides of the networks i.e. from outside or from inside of the network. These individual mobile nodes were attacked easily because of hardship of the investigation for the individual node.
- The security mechanism based on the technique of static placement is not much stronger that can prevent the network from attacks. In order to achieve the high availability for the user, a network must be employed with a dispersed mechanism that does not possess the central entity. This central server based network can be the main reason for the attack in the network.

From the collected statements it is clearly demonstrated that even applying different types of the security mechanism does not provide a network that is not vulnerable. Different steps had been taken in order to achieve a network that does not have the vulnerabilities such as applying the cryptography technique etc. From the above observations it can be concluded that nodes should not immediately trust other node. So a trust model can help to identify trustworthiness of a node. This provides the information of the capability of the node to take part in the routing process.

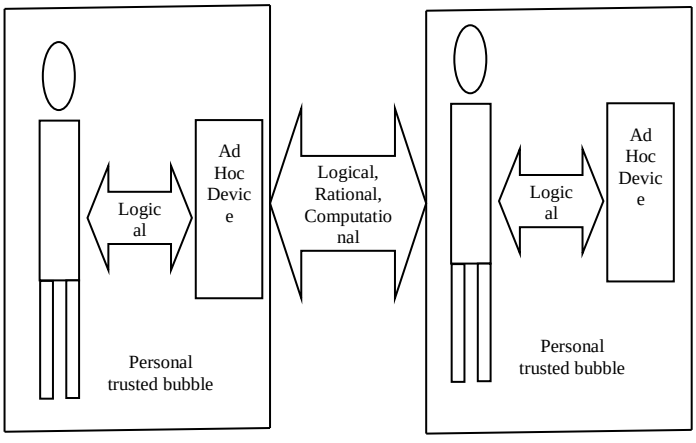

Figure 1 Independent Trust Model

Trust based modeling provides a technical method to show the digital assessment of the node in the network. These trust models can be further classified on the basis of ad hoc networking. One of the trust model is termed as independent model and shows the independent ad hoc network properties where the connection is not present with the fixed network.
Another present model is known as cross model in which limited or a few links are present with the fixed network. These two trust model shares the similarity of the presence of Personal Trusted Bubble (PTB). It shows that the main hub of the ad hoc network illogically trust in devices and based on that the actual communication takes place.

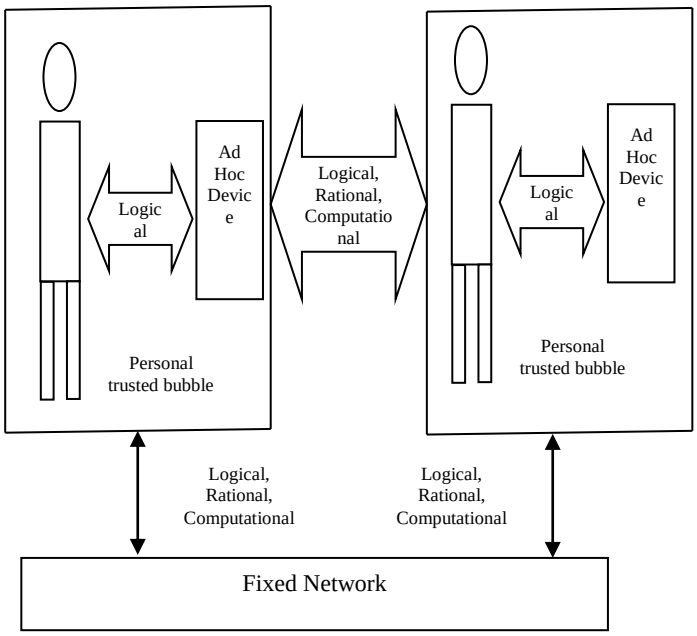

Figure 2 Cross Model

In the routing protocols an assumptions is taken that every node that is present in the network is a trustworthy node and is capable to take part in the routing process. But this is not true in all the cases, because the node that is malicious present in the network take this assumption for granted. Various types of attacks like Denial of service Attack, Man in Middle Attack and black hole can lead to the destruction of the whole network. As discussed before, the Mobile Ad Hoc Networks are not secure as it does not base on the fix physical structure mechanism.
The network based on trust shows following four main properties.

- Context Based: This represents that the node relationship based on trust in a network is meaningful in some framework.
- Function of Uncertainty: The Trust value of a node is based on the estimated probability value at the time the node performs some activity.
- Quantitative Values: This property depicts that the trust shows the discrete or continuous value only.
- Asymmetric Relationship: An asymmetric relationship is shared between the trust values of the nodes. For example if node A trusts node B it may not be possible for the opposite.

The trust model based routing concept is a derived form of human's social relationship. When a human met other human they have some interaction and just based on this interaction they come to an opinion about one another. For us if we ever met any stranger and it was needed to do any deal or business with them what we do? We collect some information about that person from some mutual connection. On the basis of this collected information, we form a decision to trust them or not. This is the same way MANET works. In MANETs there is two type of trust classifier First hand and Recommendation trust. After collaborating both these trust factors, final trust values were obtained.
This security system concentrates on trust management structure that was already discussed in the previous work [17] in order to find the malicious packet. This finding focuses on the security of the information plane by taking the genuine at the time of formation by showing the malicious activity of the node at the time of transmitting the information by eliminating the packets. Some papers concentrate on the use of trust management structure in order to achieve the secure transmission of the data. In the trust management scheme, for protection of the data when the communication is occurring, malicious packet dropper were identified and further utilized for selecting the secure path in order to establish the secure communication [19]. This is achieved by dropping the malicious packets that was identified in the earlier process of communication. We can divide Trust based security mechanism on the basis of five phases as given below:

1. Data Transmission Phase
2. Report Request Phase
3. Report Processing Phase
4. Blacklist Propagation Phase

Take an assumption that in the present network, in which each communication process have N number of packet transmitted and for the same five phases for this communication process was described:
a) Data Transmission phase: initially the source node transfers N packets and intermediate nodes broadcasts a link layer for acknowledgement of the closest node [5]. It possesses the hash value that is unique for every transfer. This attached value is then pre checked and further referred to draft a report [20].

b) Report Request Phase: In the next phase, a confirmation is generated for each node on the basis of the acknowledgement report generated for the routing mechanism [6].
c) Report Processing Phase: In this phase evaluation of the report was done for finding the nodes that are malicious packet dropper and then blacklist or ban these nodes from performing the communication in the network.

d) Blacklist Propagation Phase: In this phase an alert message is being generated for the nodes present in the network about the not that was blacklisted in the last phase [21]. That provided an opportunity to the node to recognize the node that were blacklisted and restrict them to participate in the route formation procedure.

e) Secure Route Establishment Phase: In this phase the collected information about the blacklisted nodes are inherited so the banned nodes can be dropped from the future routes. This phase is also responsible for distribution of the pre evaluated has values to the concerned nodes by the destination node.

The process of trust evaluation is one of the most important parts of the trust based security mechanism. Trust value of a packet, a node or a route is evaluated by finding a certain threshold value [22].

The figure 13 depicts the trust evaluation process.

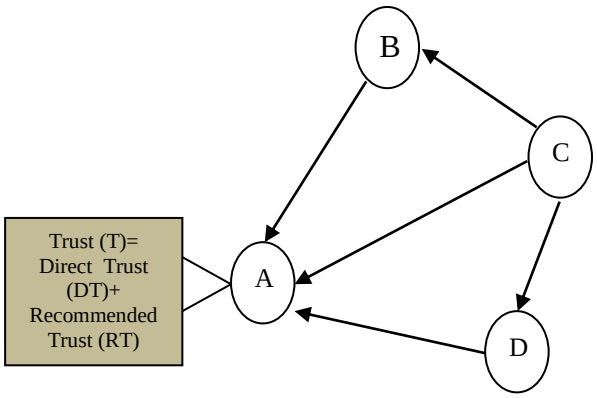

Figure 3 Trust Evaluation Process [15]

a. Direct Trust:

Direct Trust is an evaluated value for a node to the other node and is totally based of the communication process took place with the other node [23]. This concept categorizes the action of network in two forms i.e. Positive events and Negative Events. In positive events, actions like route error, route reply, route request or data flow is considered whereas in Negative events flooding, packet dropping and deletion of route were considered.

b. Recommended Trust:

In this trust form, a node providing the reference about the corresponding node is termed as the recommender node [24]. And the node about which the reference is added is termed as the recommended node. In this the route data packets are responsible to obtain the recommendations.

II. RELATED WORK

Dan-Yang Qin (2011) [6] There are enormous issues that may encountered over the communication or network path. Some of them are state route, delay and broadcast storm. In order to fight with these issues, SRS means Survival Routing Strategy has introduced. To check efficiency of the introduced technique, various evaluations methods had been introduced in terms of overhead and packet delivery ratio **H. Xia, et al (2013) [7],** To make the system secured from harmful nodes, this paper introduced a dynamic trust forecasting model so that node's authenticity can be validated. Technique used for the validation of node was based on its past operation and future behaviors and to study these behaviors different fuzzy logics were implemented for forecasting purpose. The proposed authenticity forecasting model had been in cooperated with source routing technique. This proposed network was new and based on trust features of node. In this paper, the proposed MANETs or wireless ad-hoc network was flexible and in this network feasible approach was used to determine shortest path for secured transmission of data packets. Various experiments had been done to analyse operational efficiency of proposed technique of finding the harmful nodes and making the secured network. **Kartheesan, L et al (2012) [9],** For MANETs**,** trust based Packet Forwarding Scheme was introduced by the author so that various risk factors can be reduced. This technique offers the ability to state network necessities. Author had proposed the Trust Based methodology for Combined Data Security which mainly focused on Integrity and Authentication. The trust indexes of the nodes were computed first and path was selected according to that trust value which enhanced integrity. A Distributed Certificate Authority (DCA) method was recommended for authentication in which several Distributed certificate authorities are essential to produce certificate. Thus newly introduced technique for securing the data i.e. Trust based Packet Forwarding method had provided complete security of data in MANETs communications. **Pushpita Chatterjee (2009) [15],** Author had proposed the distributed self-organizing trust based clustering technique to make the ad-hoc networks safe and secured. The mobile nodes were vulnerable to various types of attacks that can affect the security of the network. Therefore network safety guarantee plays vital role. For making the network secure, it was vital to appraise the dependability of nodes without depending on dominant establishments. In our proposal the indication of dependability was captured in a well-organized manner and from broader viewpoints including direct connections with neighbours, observing connections of neighbors and through references. For obtaining direct trust rating trust assessment algorithm was used as the prediction method for each node and it was regularized as an uncertain value between zero and one. The indication theory of Dempster-Shafer [8] used to syndicate the indications collected directly by CH (i.e. Cluster head) and the references from other neighbor nodes. Furthermore, this scheme not limited for a single gateway node for inter cluster routing. **Ranjitha.R et al (2014) [17],** There were lots of protocols recognized to shield from DOS attack, but it was not effortlessly possible. One such DOS attack was Vampire attack. On the layer of the routing protocol, this vampire attack was used as resource reduction attacks, which enduringly detach the networks by rapidly demanding nodes' battery power. These "Vampire" attacks were not precise to any particular protocol, but somewhat based on features of many general classes of routing protocols. This project exemplifies a method to bear the outbreak by employing the Cluster Head. When Vampire attack takes place, then Cluster

Head start allocating the packet in which the information is embedded to the target node and simultaneously avoid the packet drop. Therefore vampire attack would not be able to affect the efficiency of message delivery. Consider the worst scenario in which the one vampire can leads to the network-wide energy utilization by amount of O(N), Here N stands for total nodes in the network. **Shuaishuai Tan et al (2016) [20],** various attacks encountered by the data carried in the ad-hoc networks because of the features like directness and active topology. Therefore, a novel trust management method was introduced by the author to make the data secured in the ad-hoc networks. In this approach, fuzzy logic is engaged to put together in accurate practical knowledge, which is utilized for analyzing path trust value. For the provision of protection against growing attacks to trust management systems like slandering and harbouring, a filtering algorithm was proposed. An effective and reliable decay method was also projected to solve the variance about the decomposing historical trust value in a trust-based routing decision. Moreover, a potential trust factor collection method was also anticipated in this paper to ensure the compatibility of trust management system with other security constraints. At last, the proposed trust management system was implemented by integrating it into OLSR protocol. The results of evaluation represented that the recommended system performed well in the identifying and resolving data-plane attacks. **X. Anita, et al (2014) [25],** The obliging environment of multi-hop wireless sensor networks (WSNs) made it susceptible to diverse types of attacks. The subtle application environments and resource boundaries of WSNs command the necessity of lightweight security scheme. The earlier security resolutions were based on ancient behavior of neighbor but the safety can be improved by forecasting the upcoming behavior of the nodes in the network. In this paper, a fuzzy-based trust estimate model for routing (FTPR) in WSNs with negligible overhead in regard to memory and energy ingesting. FTPR integrates a trust prediction model that guessed the future behavior of the neighbor based on the historical behavior, variations in trust value over a period of time, and reference discrepancy. In order to decrease the control overhead, FTPR received commendations from a subsection of neighbors who had supreme number of interfaces with the requestor. Theoretical examination and imitation consequences of FTPR protocol validate higher packet distribution ratio, and energy ingesting than the traditional and current trust-based routing schemes.

Table 1: overview to the related work

S. No.	Paper	Author Name	Objectives
1.	A Trust Management System for Securing Data Plane of Ad-Hoc Networks	Shuaishuai Tan et al [20] (2016)	The objective of this study was to establish a trust based security technique in which the OLSR routing protocol and fuzzy logics were implemented system. This approach secures the data planes from various attacks.
2.	Trust based routing mechanism for securing OSLR-based MANET	Shuaishuai Tan et al [22] (2015)	This study was conducted to establish the objective to develop secured technique for MANETs by implementing concept of fuzzy based trust value and then this collaborate this with OLSSR and were named as FPNT-OLSR.
3.	Secure Wireless Ad-Hoc Sensor Network from Vampire Attack Using M-DSDV	Ranjitha R et al [17] (2014)	This study was conducted to prevent the network from Denial of Service attacks particularly vampire attacks. Since specific secure routing protocol is not suitable to detect this attacks hence the in this work author implements the cluster heads and then these cluster heads transmits the packet containing information to the target node even when the vampire attack occurred in asd-hoc network. In the worst case, a single Vampire can upsurge network-wide energy usage by a factor of O(N), where N was the number of network nodes.
4.	Security enhancements for	Z. Wei et al (2014)	The proposal given by this

	mobile ad hoc networks with trust management using uncertain reasoning	[27],	study was to develop a secure routing protocol for MANETs that evaluates both direct and indirect trust values. The direct trust value was resulting by using Bayesian theorem whereas indirect trust value was resulting by using dempster shafer algorithm.

The routing can be achieved by using various routing techniques. There are many routing techniques developed that can help to generate the efficient path for communication. But all the traditional routing techniques select the route on the basis of shortest distance. Only single parameter is considered by the traditional routing techniques that is shortest path finding. In these techniques first of all the possible routes are generated from source node to sink node and then the path with the shortest distance is selected as an efficient path for routing. The lacking side of these techniques is that these algorithms are not that efficient. Therefore, it becomes necessary to develop such a mechanism which can answer the shortcomings of previous routing algorithms.

Large amount of modern ad-hoc networks have the ability to work in both directions and also activate the management of sensor activity. As ad hoc networks are based on dynamic topology system hence it may suffer different types of attacks on the data carried in its network. Worst thing is that few attacks can bypass the frequent identity based security techniques. Therefore securing data carried in ad hoc network, the [22] trust management system has been introduced. In this the fuzzy logic was used for evaluating the path by evaluating the trust value using average delay and PDR. Hence there is a requirement to enhance this work since the parameters considered for evaluating the trust value are sufficient to achieve the highly efficient output.

II. CONCLUSION

This paper discusses the routing methods and present security challenges for the route selection. As studied in the previous literature, different security techniques were applied for routing such as OLSR, Fuzzy logics, MANETs etc. In this paper different literatures related to routing have been studied that tried to achieve the security and trustworthiness. Most of the authors tried to achieve the secure route finding method and trusted next hop selection but no system is present that defines the trustworthiness of the next hop. So there is a need to develop a system that defines the trustworthiness of the next hop in order to select the trusted hop and improve the secure transmission within the network.

REFERENCES

[1] Alex Hinds, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)",IJIET, Vol 3, Pp 1-5, 2013

[2] Ashish Kr. Shrivastava et al, "Study of Wormhole Attack in Mobile Ad-Hoc Network", International Journal of Computer Applications, vol 73, Issue 12, Pp 32-37, July 2013

[3] Bijender Bansa et al, "Attacks Finding and Prevention Techniques in MANET: A Survey", IEEE, Wired and Wireless Communications Vol.4, Issue 2, Pp 1-7, 2015

[4] Bing Wu et al, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", SPRINGER, In *Wireless network security*, pp. 103-135. Springer US, 2006

[5] Charu Wahi, "Mobile Ad Hoc Network Routing Protocols: A Comparative Study", IJASUC, Vol 3, Pp 21-31,2012

[6] Dan-Yang Qin ,"An Effective Survivable Routing Strategy for MANET", 2011

[7] H. Xia, et al., "Trust prediction and trust-based source routing in mobile ad hoc networks", IEEE, Ad Hoc Netw., vol. 11, no. 7, pp. 2096–2114, Sep. 2013.

[8] I. Aad, et al "Impact of denial of service attacks on ad hoc networks", IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. 2008.

[9] Kartheesan, L et al, "Trust Based Packet Forwarding Scheme for Data Security in Mobile Ad Hoc Networks", OSR Journal of Computer Engineering (IOSRJCE) 2278-0661 Volume 2, Issue 3, PP 40-48, July 2012

[10] Lidong Zhou et al, "Securing Ad Hoc Networks", IEEE, Pp 1-12, November 1999

[11] Muhammad Imran, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science, Pp: 384-390, 2015.

[12] M. Marimuthu et al, "Enhanced OLSR for defence against DoS attack in ad hoc networks", J. Commun. Netw., vol. 15, no. 1, pp. 31–37, Feb. 2013.

[13] Pooja Pilankar et al, "Trust based security in manet", IJRET: International Journal of Research in Engineering and Technology, 2319-1163, Volume: 05 Issue: 02 , Pp 12-19, Feb 2016

[14] Prosenjit Bose, "Routing with Guaranteed Delivery in Ad Hoc Wireless Networks",Wireless Network, Vol 7, Pp 609-616, 2001

[15] Pushpita Chatterjee, "TRUST BASED CLUSTERING AND SECURE ROUTING SCHEME FOR MOBILE AD HOC NETWORKS", International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, Pp 84-97, July 2009

[16] P. F. Saverio, A. Detti, C. Pisa, and G. Bianchi, "A framework for packet droppers mitigation in OLSR wireless community networks," in Proc. IEEE ICC, pp. 1–6. 2011

[17] Ranjitha.R et al, "Secure Wireless Ad-Hoc Sensor Network from Vampire Attack Using M-DSDV", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, pp 4081-4087, May 2014

[18] Savitha. M et al, "A Study on Various Attacks in Wireless Ad hoc Sensor Network", International Journal of Computer Science and Mobile Computing, vol 3, issue 9, pp 231-243, September 2014

[19] Sayan Banerjee, "A Review on Different Intrusion Detection Systems for MANET and its Vulnerabilities", IEEE, 2015

[20] Shuaishuai Tan et al, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks", IEEE, transactions on vehicular technology, vol. 65, no. 9, pp 7579- 7592, September 2016

[21] Sudha Dwivedi et al, "Review in Trust and Vehicle Scenario in VANET", IEEE, Future Generation Communication and Networking Vol. 9, No. 5, pp. 305-314, 2016

[22] Shuaishuai Tan et al, "Trust based routing mechanism for securing OSLR-based MANET ", ELSEVIER, Adhoc Networks, March 2015

[23] Tameem Eissa et al, "Trust-Based Routing Mechanism in MANET: Design and Implementation", SPRINGER, Mobile NetwAppl, Pp 1-12, June 2011

[24] Vanita Rani et al, "A Study of Ad-Hoc Network: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol 3, Issue 3, Pp 135-138, March 2013

[25] X. Anita, et al, "Fuzzy-Based Trust Prediction Model for Routing in WSNs", HINDAWI, Volume 2014 (2014), Pp 1-11, July 2014

[26] Xiaocong , "TIGHT: A Geographic Routing Protocol for Cognitive Radio Mobile Ad Hoc Networks",IEEE,Vol 13, Pp 4670-4681,2014

[27] Z. Wei etal, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning", IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4647–4658, Nov. 2014