A REVIEW: TRUST, ATTACKS AND SECURITY CHALLENGES IN MANET

Ashish kumar khare[1], Dr. R. C. Jain[2] and Dr. J. L. Rana[3]

[1] PhD Scholar, SATI, Barkatullah University Bhopal, India
[2] Ex-Director, SATI, Barkatullah University Bhopal, India
[3]Ex-HOD, CSE, MANIT, Bhopal

ABSTRACT

Mobile Ad-hoc Networks or MANETs are mostly found in situations where any fixed facilities are just not available. MANET provides some fundamental responsibilities such as routing, packet forwarding communication and network management etc over self structured network. This specially affects the energy, bandwidth and memory computation requirements. Providing trust in MANET is an additional critical task because of lack of centralized infrastructure. Since during the deployment of MANET nodes that are fresh continue returning and aged ones go from the cluster/network, there is demand for maintaining the record also to provide appropriate certification for the arriving node(s) that are fresh as well as the present node(s) in the network. But due to various types of intrusion threats and attacks it is hard to fully scrutinize any new node so as to allow only safe nodes to get connected with the existing safe system. In a cluster of large size these trusted node(s) will likely be communicating together, all the while allowing or disallowing entry/communication of the compromised node(s) or trusted model to continue to maintain a stable, secured, trustworthy group of movable nodes. All the reported techniques have been systematically categorized and their strong and weak points have been discussed.

KEYWORDS

Attacks, MANETs, Security, Trust, Wireless network.

1. INTRODUCTION

A MANET is a highly capable and fast deployable wireless network technology. It is primarily based on a self organized and rapidly used network. The network is a self-organized means that all network operations- discovering the topology and delivering data packet must be executed by the node(s) themselves and that its routing operation will be integrated into mobile node(s). MANET is challenging and innovative areas of wireless networks. Due to its immense features, MANET is very useful to real world application areas where the networks structure/topology changes very rapidly [1]. Node(s) in MANETs may leave /relieve and may join/rejoin the network dynamically because node(s) change their position over time. There isn't any centralized administration and permanent group of infrastructure in this kind of networks. Due to dynamic nature MANETs are highly vulnerable to different attacks. One of the basic necessities for a secured MANET is use of secure protocols which ensure the network integrity, confidentiality, availability and authenticity. Most of the security solutions of wired networks do not effectively work for MANET environment. As the communication occurring in open method makes the MANETs more susceptible to security attacks[4]. By using security protocol, affect of various attacks can be reduced. The mobile hosts dynamically discover route among one another so that they can convey messages for connecting. Success of communication depended on the co-operation of the complex mobile node(s). The evolution of wireless networks plays vital roles in new society. Limitations of infrastructure, self organization and dynamic change of node(s) are the main characteristic of Mobile Ad Hoc Network. The major challenge of MANET is the

DOI : 10.5121/ieij.2015.3301

vulnerability to security attacks [2] [16]. The security dispute has become a prime concern to provide secure communication in MANET.

This paper is organized into six parts as following. *Section 1* presents the history of the topic: Special features of mobile ad hoc networks. Section 2 Concentrates on TRUST, types of TRUST and its characteristics. Section 3 discusses Attacks and its type. Section 4 provides security issues/difficulties encountered when the conventional networking strategies are used in MANETs. Section 5 provides related works giving an overview of the existing remedies for MANETs and discusses the applicability of the security design. Finally, section 6 Proposes conclusion and future research potential for securing in MANETs.

2. TRUST IN MANET

Trust is considered by a basic description to be a measure of subjective opinion that one party or person uses to evaluate the probability that other person or party will execute a favorable action when the opportunity presents itself and to observe whether that motion has occurred. Whenever intended to facilitate with high-probability the activities one person or party are expected to execute will be done in a manner which is advantageous. When making trust associations among participating nodes it is critical to enable collaborative optimization of program metrics. This notion is crucial to communication and network functional designers. [13][15]. A key consideration that outlines the importance of the subject in relation to the security of Mobile Ad-hoc Networks (MANETS) is that trust is always required in developing relationships when there is uncertainty. This is in line with the problem of MANETs where the unforeseen behaviour is a key concern. A Trust can also be defined as behaviour of a group of associations among things that contribute in a process, in which these associations are on the basis of the proof created by the earlier communications of entities. Trust may occur between these entities, in the event the communications happen to be true to the process afterward. In another way trust is the amount of faith in regards to the behavior of additional things (representatives).In MANET trust can be defined as a level of belief according to the behavior of nodes (or agents ,entities etc).The probability value of trust varies from 0 to1, where 0 stand for DISTRUST and 1 stand for TRUST [9].

A. Characteristics of Trust in MANETs

Due to wireless medium of MANETs, characteristics and the theory, trust must be cautiously defined.[18] Trust in MANETs essential feature is as follows:-

1. A decision technique to verify trust toward an entity has to be fully spread because the being of a trusted third party (example a trusted central certification authority) cannot be supposed.
2. Trust must be confirmed in a well customizable way without too much communication load and computation, even while capturing the intricacies of the believe association.
3. A decision support for MANETs must not believe that node(s) are co-operative. In selfishness and resource-restricted environments it is likely to be widespread above collaboration [9].
4. Trust can't be static. It is dynamic.
5. Trust is subjective.
6. Trust is not basically transitive. The reality is that X trusts Y and Y trusts Z does not imply that X trusts Z.
7. Trust is considered as asymmetric but essentially it is not reciprocal.
8. Trust is context-dependent. X may trust Y in one aspect but, not in other aspect.

In MANETs, most of the node(s) participating in routing ,requires high computational power as such the node with high battery power is regarded as trusted while a node that has low battery power but is not malicious (i.e., honest) is distrusted.

B. Centralized Versus Decentralized Trust

Centralized trust refers to the state in which for each additional node in the system trust values are calculated by a worldwide trusted node. All user node(s) of the method request this trusted node to provide them with advice about additional node(s).The state explained here has two main implications. First, it's reasonable to suppose that distinct user node(s) are likely to have dissimilar opinions regarding the same target node. Secondly every user node dependents upon the trustworthiness of this node that is single, thus revolving it into just one point of failure. This fact is covered up in decentralized scheme of the trust issue where a node communicates to every user node thus being the center of its own world. i.e., user node(s) are accountable for computing their very own trust values for almost any target_node they desire. This "bottom-up" approach is most widely implemented [14][15].

3. ATTACKS IN MANET

Attacks on network come in various varieties and they can be grouped based on unusual characteristics. Many researchers used special aspect to classify the attacks on MANET. The researcher classified the attack based on the trustworthiness of associate node(s) in the network [5][11]. They separated the attacks on MANET into different categories. These attacks can be classified as a passive or active attack.

A.Passive vs. active attacks

Passive attacks are started by attackers to steal useful information from the targeted networks. Case of passive attacks in MANETs is eavesdropping attacks and traffic analysis attacks. These kind of attack are almost impossible to find because neither the method resources nor the crucial network features are physically affected to prove the intrusions. While attacks that are passive don't want to interrupt or disrupt the network operations, attacks that are energetic on the other hand, actively alter the data with all the intention to block the operation of the targeted networks [6]. Here some active and passive attacks are discussed :-

3.1 ACTIVE ATTACKS

3.1.1 Black hole Attack

In a black hole attack, an advertisement of a zero metrics is made by attacker to all nearby destinations. Thus creating all fictitious nodes in the region of it to route packets. False routing information is sent by malicious node, asserting that it has an optimal route which causes other normal node(s) to route data packets through one which is malicious and that node drops every packets that it receives for forwarding those packets normally. In this way an attacker causes abnormal delivery of packets. An attacker pays attention to requirements in a flooding based protocol [7].

3.1.2 Wormhole Attack

A more clever type of active attack is the formation of a tunnel between two joined malicious node(s).This is a kind of link via a private network connection, and which replaces normal link

in the network, disrupting normal routing gets disrupted. The tunnel between two joined nodes is referred to as a wormhole. Wormholes are unsafe and identification of Wormholes is very difficult. This uses nodes to short-circuit the normal flood of routing message, creating a effective peak cut in the network that is controlled by the two joined attackers [4].

3.1.3 Rushing attack

The tunnel process is shared by two in similarly committed attackers to a wormhole. In case a rapid communication path (e.g. a committed channel used by committed attackers) resides in between the two end points of the wormhole, the tunneled data packets can disperse comparatively faster than those via a standard multi-hop route. The rushing attack can behave as a successful denial-of-service attack inspite of all presently planned on-demand MANET routing protocols like AODV, DSR and including those protocols that have been designed to be secure, such as Ariadne and ARAN [4].

3.1.4 Byzantine attack

An arrangement of set of intermediate node(s) working safely inside the network may bring attacks likewise by making routing loops to forward data packets via non optimal paths or randomly dropping packets which leads towards interruption of routing services inside the network [16].

3.1.5 Replay attack

In the replay attack attacker disrupts the network routing traffic by continuing to retransmit the genuine data repeatedly which have been captured before. This attack generally targets the newness of routes, but it is also very useful to test the weakly designed security solutions of networks [4].

3.1.6 Flooding

In this attack destructive nodes inject fake packets into the network, or create ghost packets that curl about due to wrong routing information, efficiently causing depletion in the information measure and process resources. This has particularly significant impact on networks that are unplanned, since the nodes of those ordinarily possess entirely restricted assets concerning battery and process power. Traffic also can be a problem like financial issue, gambling on the services provided, causing data_flood that hits up the traffic data of a malicious node or resulting into significant system disruptions.

3.1.7 Location disclosure attack

In this attack an attacker first observes the node Location and layout of whole networks. It refers the traffic analysis methods and monitoring approaches to know much about the destination node and network. Antagonist tries to seek out the characteristics of communicating node(s) and examine traffic to understand network traffic prototype and path changes. The outflow of this information is a severe security breach.

3.1.8 Sinkhole

In this kind of attack, a compromised node attempts to bring the data from many neighboring nodes to itself. The attacking node attempts to provide a very appealing link. So, plenty of traffic passes this node. Each of the data that's being conveyed between the neighboring nodes is

eavesdropped by it. These attacks also can be executed on Ad-hoc networks by AODV protocol using computation for reducing the hop count or maximizing the sequence number, therefore making the trigger route offered through the malicious node is apparently the most effective available route for the node(s) to convey [11].

3.1.9 Spoofing Attack

In this attack, the attacker assumes the identity of some other node in the network; consequently it gets the messages which are intended for that other node. Such attack could be made by any destructive node(s) that have sufficient information of the system to invent a fake identification of one of its associate nodes. Using that ID as a bonus, this node may misguide additional nodes to create paths towards itself as opposed to towards the first node [11].

3.1.10 RERR Generation

When the messages are flooded into the network dislocation of several routes between different nodes in the network can be caused resulting in number of link failures. Malicious nodes may stop communications with in the network by delivering RERR messages to some node across the route.

3.1.11 Sybil attack

Network scenario that is dispersed is specially aimed at by the Sybil attack. The opponent intends to do something as a number of different details/nodes as opposed to one. This permits the attacker to falsify a vote useful for threshold protection methods' consequence. [6].

3.1.12 Jamming

In jamming, opponent initially keeps tracking wireless medium so as to find out frequency at which location node is receiving signal from transmitter. Attacker afterward transmits signal on such frequency to ensure malfunctioning of reception [4].

3.1.13 De-synchronization attack

In this attack, the affected node repeatedly sends the wrong messages for retransmission to over a pair of nodes (source and destination).Such wrong message are transmitted again and if the affected node manages the things. These wrong “retransmit “message are exchanged back and forth thus causing energy depletion of legitimate nodes and consumption of network bandwidth in endlessly, invoking synchronization recovery protocol. [3].

3.1.14 Overwhelm attack

In this type of attack, a community node may get drowned due to large volumes of traffic, sent by a source node. This attack consumes destination node energy and network bandwidth [3].

3.1.15 Blackmail

This attack occurs against routing protocols that use recognition mechanisms. It behaves that are like Pathrater and Watchdog. Affected node might use valid nodes to be blackmailed by these mechanisms to stimulate additional nodes that appear authentic to set of valid nodes [19].

3.1.16 Denial of service (DoS) attack

The assaults are aimed at interruption of entire network operation and routing information of ad-hoc network. DoS attacks disrupt the networking functionalities without any interruption of security threats [6].

3.1.17 Gray-hole attack

This attack is routing misbehavior resulting into failure of communications. It consists of two stages. One of the stages is node marketing itself as having a valid path to destination node. In the second stage nodes intercept packet using a specific match [6].

3.1.18 Selfish Nodes

In this attack there is a node not forwarding/ exchange's the message to other nodes which are in the network. Network services are not supported by this destructive node. Node that is selfish utilizes the network for its benefit i. e to conserve its power [2].

3.1.19 Man-in-the-middle attack

It is like an opponent seated between the transmitter and recipient and absorbs any information being delivered between the pair of nodes. In this attack, opponent can mimic the transmitter to communicate with recipient or mimic the recipient to respond to the transmitter [6].

3.1.20 Fabrication

The terminology "fabrication" is employed while talking about attacks done by creating fake routing communications. Attacks come as legitimate routing concepts and create routing error messages, stating that the neighbor cannot be called [15].

3.1.21 Impersonation

Impersonation attacks are initiated through the use of the identity, such as MAC-address or IP address of other node. In this attacks are generally the initiatives for the majority of other attacks. This type of attack is employed to launch further, more complex attacks [19].

3.2 PASSIVE ATTACKS

3.2.1 Traffic Monitoring

It is used to recognize the communicating events and performance which in turn may advice malicious node to launch additional attacks. It is not unique to MANET only, additional wireless network including satellite, cellular and WLAN additionally suffer from these possible exposures [11].

3.2.2 Eavesdropping

The phrase eavesdrops means overhearing without investing any additional effort. This is studying conversation or information by unintended recipient. In MANET a wireless method is shared by mobile host. The majority of the communication that is wireless uses RF spectrum. In the process of transmitting, message might be eavesdropped and false message might be injected into network [6].

3.2.3 Traffic Analysis

Visitor's analysis is a kind of passive attack. It is used to get information about node(s) by talking to every other node and also analyzing how much of this information is refined.

3.2.4 Sync flooding

This type of attack is denial-of-service attack. An attacker can frequently make fresh link appeal until the resources demanded by every connection reach a limit or exhausted. It creates serious resource restrictions for nodes that are valid.

B. External vs. internal attacks

Outside attacks are attacks started by opponents that aren't initially approved to participate in the network operations. This kind of attacks is typically planed to cause network congestion, to disrupt the network procedures that are put on hold or refusing access to particular network operation. Denial of service (D0S), fake packets injection, and copy of messages are some of the attacks that are frequently initiated by the external attackers. Additional attacks in the MANETs might appear from another source, which is the interior attack. Internal attacks are initiated by the authorized nodes in the networks, and may appear from both misbehaving nodes and compromised nodes [4].

4. SECURITY CHALLENGES

There are different security challenges in MANET namely:

1. Channel Vulnerability**:** Broadcast Wireless using medium allows easy message Eavesdropping and Injection.
2. Node Vulnerability**:** Nodes do not operate from physically protected places, thus easily fall under attack.
3. Absence of Authentication Authorities /Infrastructure/ Certification.
4. Dynamic changes in Network Topology and security threat under the routing protocols.
5. Computational and Power Limitations prevent the use of complex Encryption Algorithms.

In MANET protection some investments which can be significant are required. This may cover all networking capabilities including packet forwarding and routing, perform by nodes in a self organizing way. Totally protecting a MANET is extremely difficult [3][17][18].The objective to evaluate if ad hoc network is safe are as follows:

4.1 Availability:

Availability indicates that the resources are accessible to certified parties at times they are needed. Accessibility is used to both services and also to data. It ensures survivability of network support even under denial of service (DoS) attack.

4.2 Confidentiality:

Confidentiality helps to ensure that pc-related resources are obtained only by approved parties. i.e., just those who must have use of something will really get that access. The confidential information need to ensure that confidentiality may possibly be kept secret from all entities. Secrecy doesn't have freedom of right to use them. Confidentiality might be called privacy or secrecy.

4.3 Integrity:

Integrity indicates the manner that is only official or that resources may be changed only by authorized parties. Change includes removing or writing, shifting position. Integrity ensures the information being transmitted is never altered.

4.4 Authentication:

Authentication enables a node to make sure member node's identity it is communicating with. Authentications essentially guarantee perhaps not impersonators and that individuals in communicating are authenticated. Credibility is guaranteed as the valid sender may generate an message that can decrypt correctly using the key that was shared.

4.5 Non repudiation:

Non repudiation helps to ensure that transmitter and recipient of a message can't deny they've actually delivered or received this type of concept. This is useful when we should discriminate in case a node among several unwanted role is compromised or maybe not.[3]

4.6 Anonymity:

Anonymity / ambiguity indicates all information which can be employed to identify current or owner user node(s).Information about such node(s) must be held personal and should not be scattered by the network device/software or node itself. [3]

4.7 Authorization:

This assigns distinct access rights to different kinds of users. For example network administration may be carried out only by network administrator exclusively [9].

5. RELATED WORK

Because of amazing characteristics, dissimilar actual world uses areas where the networks topology changes quickly in MANET. Several investigators want to eliminate computational constraint of MANET like, battery power, limited bandwidth and security ability. A great deal of function under improvement in this topic particularly redirecting its particular existing counter measures and attacks. Today's protection options of wired systems can't be practical right to wireless network, making a MANET significantly more susceptible to security attacks. In this study, we've discussed assaults prevalent in MANET. Some options that rely on key management and cryptography have also been discussed.

Recently several models and algorithms have been proposed to improve security in MANET.
Dr. B.S. Pradeep et.al [8] proposed an application of Artificial Neural Network (ANN to mobile Ad Hock Network) for multicasting where the problem is to find an efficient route to transmit packets over many nodes in the network. Authors have proposed effective and novel application of Artificial Neural Network to Secure Multicasting in MANET with supporting Nodes. This has gained a lot of attention for secure routing using an ANN model.

Suresh Kumar et.al [10], have proposed control packets to determine the routes between for sources and destination nodes. The proposed algorithm adapts rapidly to routing changes when host movement is frequent. In Node Transition Probability (NTP) routing algorithm, route is discovered using the received power at a particular node from all other nodes. NTP along with the fuzzy logic for routing is less promising because they are too costly for resource controlled in MANET. They still may not be ideal in regard to trade-offs between efficiency and effectiveness.

Some alternatives work nicely in the presence of one compromised node, but they could not be relevant for multiple attackers which are colluding.

Reijo M. Savola et.al [11] have proposed a flexible security measurement framework model for MANETs, that is useful for different mode of security measurement like off-line security metrics and on-line security monitoring mechanism .The system works on different component of network like network-level, node-level and network segment-level .Security level of the system is based on measurement of trustworthiness and confidence of the node.

H.Hallani et.al[12] have Proposed a trust based approach to improve security between Node(s) using fuzzy logic. To mitigate the cause of malicious node(s) and to achieve higher levels of security and consistency, they have developed an appropriate fuzzy logic concept to propose an algorithm to set up quantifiable trust levels between the node(s) in Ad-hoc networks. Trust levels are then used in routing decision making conception. This is efficient in determining the most secure route during the routing discovery.

H.Yanget.al [16] have designed a personal-procuring strategy, in which several node(s) collaboratively provide certification solutions for different node(s) within the network. Multiple node(s) which require a local model that sets the foundation for the layout was formalized first. Authors have also suggested a model refined localized process that additionally takes the trust level from a certification provider which in turn infers the level of trust of neighboring nodes. The proposed process is scalable and has built in mechanism to up and down grade the trust level of nodes periodically based on their behavior.

6. CONCLUSION AND FUTURE WORK

Since MANETs have dynamic infrastructure and no centralized management they are very susceptible to several types of attack. In this paper, we have discussed Trust, security challenges and different types of attacks in MANET. Different security mechanisms are compared in order to check their effectiveness in handling network problems. Most previous and recent ad hoc networks have already focused on providing routing services without considering any high level security and Minimum delay Mechanism. To provide the solution for secure communication and minimum delay in mobile ad hoc network, research direction will be focused on capabilities on ANN and co operation of neighboring nodes. In order to determine the most secure route under constraint and to maintain trusty environment, most techniques acquire information about the neighboring node.

REFERENCES

[1] M.M.Alani, (2014, Nov) "MANET security: A survey", In International conference on Control System, Computing and Engineering (ICCSCE'14) IEEE pp. 559-564.

[2] Ben Chehida Douss, Abassi R and Guemara EI Fatmi (2014, Sept) "A Trust Management Based Security Mechanism Against Collusion Attack In a MANET Environment", In International conference on Availability , Reliability and Security (ARES'14) IEEE pp. 325-332.

[3] Ali Dorri, Seyed Reza Kamel and Esmail kheyrkhah, (2014, Feb) "An Analysis of Security Challenges in Mobile Ad Hoc Network", In International Journal of Computer Engineering & System (CSEIT) pp. 359-365.

[4] C.Sreedhar, Varun Verma Sangaraju, (2013, Oct) "A Survey On Security issue IN Routing IN MANETS", In International Journal of Computer Organization Trends Volume 3 Issue 9(IJCOT) pp. 399-406.

[5] Renu Dalal, Manju Khari and Yudhvir Singh (2012, April). "Different Ways to Achieve Trust in MANET".International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 2, No. 2.

[6] Gagandeep, Aashima, Pawan Kumar, (2012, June)"Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Vol.1, No.5.

[7] Pramod Kumar Singh and Govind Sharma (2012, Dec) "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[8] Dr.B.S.Pradeep and S. Soumya (2011, July) "Role of ANN in Secured Wireless Multicast Routing during Dynamic Channel Allocation for User Demanded Packet Optimality" Int. J. Advanced Networking and Applications pp. 1135-1139, Vol. 03, No. 2.

[9] Jin-Hee Cho and Ing-Ray Chen" (2011, Oct) A Survey on Trust Management for Mobile Ad-Hoc Networks" IEEE Communications Surveys & Tutorials, Vol.13, No. 4.

[10] Suresh Kumar, Machha. Narender, and G. N. Ramesh, (2010, Sep), "Security Provision For Mobile Ad-Hoc Networks Using Ntp & Fuzzy Logic Techniques", Global Journal of Computer Science and Technology pp. 62, Vol.10, No. 8.

[11] Reijo M. Savola and HabtamuAbie (2009, Sep) "On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks" Journal of Networks, pp. 65-379, Vol.4, No.7.

[12] H.Hallani and A.Hellany, (2009, Dec) "Wireless Ad-hoc Networks: Using Fuzzy Trust Approach to Improve Security between Nodes", In International conference on Computer Engineering & System (ICCES'09) pp. 359-365.

[13] P.B.Velloso, R.P.Laufer, O. C.M.B.Duarte, and G. Pujolle. (2008, July) "Analyzing a human-based trust model for mobile ad hoc networks", in IEEE Symp. Comput. Commun., Marrakech, Morocco.

[14] P.B.Velloso, R.P.Laufer, O. C.M.B.Duarte, and G. Pujolle, (2008, August) "A trust model robust to slander attacks in ad hoc networks", in IEEE International Conf. Comput. Commun. Netw. ANC workshop, Virgin Islands, USA.

[15] V. Balakrishnan, V. Varadharajan, U.K.Tupakula and P. Lucs. (2007) "Trust and Recommendations in Mobile Ad hoc Networks", Proceedings of International Conference on Networking and Services (ICNS 2007), Athens, Greece, pp. 64-69.

[16] YIH-CHUN HU, ADRIAN PERRIG and DAVID B.JOHNSON (2005, NOV) "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, Springer Science.

[17] H.Yang, H.Luo, F. Ye, S.W.Lu and L Zhang, (2004, FEB) "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, pp. 38-47, vol. 11, No. 1.

[18] Z.Liu, A.W.Joy and R.A.Thompson (2004, May) "A Dynamic Trust Model for Mobile Ad Hoc Networks", Proceeding of 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, Sushou, China, pp. 80-85.

[19] K.Sanzgiri (2002, Nov) "A Secure Routing Protocol for Ad Hoc Networks", Proc. 2002 IEEE International Conf. Network Protocols.