International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 9157-9165

http://www.ripublication.com

Review on Security Enhancement Methods Using Trust Management In MANETS

Hepzibah Golda.M [1], Amrutha V[2].
[1]*Student of Post-graduation,* [2]*Assistant Professor*
[1, 2] *Department of Electronics and Communication, Sathyabama University, Chennai-119, India.*

Abstract

Mobile ad-hoc networks (MANETs) are used in the field of military battle field, personal area networks, sensor networks, command sector, etc. MANETs suffer from several security issues due to their dynamic nature and the characteristics of the open air medium. Direct Observation and indirect observation are the two components of trust management that enhance security in MANETs. Trustworthiness of the node is calculate from the direct and indirect observation. This paper discusses various characteristics of MANETs, Security Goals and Trust Management based on the Literature Survey which explores various trust management methods used to increase security.

Keyword: MANET, Security, Trust, Trust management

Introduction

A mobile ad-hoc network (MANET) is a collection of independent mobile nodes that can communicate with each other. These networks are fully distributed and work at any place without the help of any fixed infrastructure.

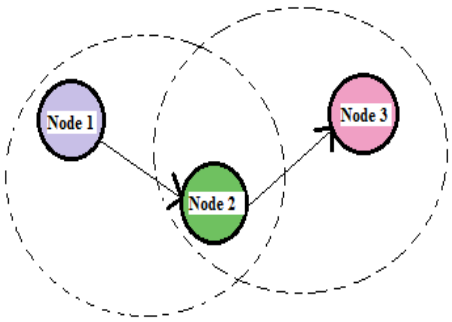

Figure 1: A Simple MANET

When one or more nodes deliver packet then it is a multi-hop routing. In MANET each node acts as a host as well as router.

A.Characteristics of Manet

i).Dynamic Topology:
The nodes are free to move with different speeds and thus the structure of the network changes randomly.

ii).Energy Constrained Operation:
The devices in the modern electronics world completely rely on batteries. The design of the network is to be optimized to conserve the energy consumed by the mobile nodes.

iii).Limited Bandwidth:
The bandwidth of the wireless network is very much limited and the network is to be optimizing to perform with the maximum efficiency within the limited bandwidth.

B.Security Goals In Manet
There are some basic security criteria to provide security in MANET

i) Authentication:
The node must know the identity of the peer node it is communicating with. Without authentication, an attacker can gain information and interfere with other node.

ii) Confidentiality:
It is to ensure that certain information is never disclosed to unauthorized entities.

iii) Integrity:
It is to ensure that the message being transmitted is not corrupted.

iv) Non-Repudiation:
The sender cannot later deny sending information and the receiver cannot deny the reception.

v) Availability:
Node should be available for communication at all times. A node need continue to provide services despite attacks.

vi). Detection and Isolation:
MANETs require a protocol that can identify the misbehaving nodes and render them unable to interfere with routing.

Due to characteristics like dynamic topology, lack of centralized authority, insecure medium, etc., MANETs become vulnerable to many number of attacks and security becomes a major issue. When a MANET is used in a military application

without security, the nodes in the network are vulnerable to attacks. There are two types of attacks; they are active and passive attacks. In a passive attack, a packet containing secret information may be eavesdropped which leads to lack of confidentiality. Active attack includes deleting a packet, modifying the original content of a packet, etc. Thus the node suffers from the lack of availability, integrity, authentication and non-reputation.

Key management which is a prevention based technique is not suited for distributed networks. To delete the selfish and malicious nodes, Trust Management scheme is introduced. In MANETs high level security can be ensured by intrusion detection and continuous authentication.

C.Trust Management

The word trust refers to the relationship between neighbouring nodes in terms of trustworthiness. Integrity, timeliness and reliability are improved by trust. Trust management includes trust establishment, trust update and trust revocation. Trust Management &Trust establishment are interchangeable. Trust establishment is the process of maintaining and distributing the trust. Trust in MANET should be self-organized in a reconfigurable way. Trust management is of dynamic nature and not static.

Classification of Trust Management:

Trust Management is classified as

- Evidence based method
- Monitoring based Method.

Properties of Trust Management:

Trust Management has some important properties which are:

- Dynamicity
- Subjective
- Asymmetry
- Context dependency

Figure 2: Properties of trust in MANET

Related Work

F. R. Yu, H. Tang et al [1] discussed about the combined design of security and QoS. QoS could be improved by cooperative communication in mobile ad-hoc Networks

(MANETs). The idea behind this was that single antenna mobile nodes in a Multi-user Scenario could share their antennas in a manner that created a virtual multiple -input and multiple-output (MIMO) system. Game-theoretic approach quantitatively analyzed the attack strategies of the attacker so as to make a rational decision on relay selection and the authentication parameter adaptation to reach an equal balance between security and QoS in co-manets.

Q. Guan, F. R. Yuey et al [2] proposed a combined design for authentication and topology control scheme for cooperative communication. In that, topology control method was designed in a combined way as upper layer security schemes and physical layer schemes related to channel conditions and relay selections to maximize the throughput. When security and throughput was considered as separate the overall performance could not be achieved.

S. Bu, F. R. Yu, et al [3] proposed a structural model to overcome the disadvantage of continuous user authentication. Continuous user authentication was an important prevention-based approach to protect high security mobile ad-hoc networks (MANETs). On the other hand, to effectively reduce the malicious activities, intrusion detection systems (IDSs) were also important in MANETs. Considering these two approaches jointly was effective in optimal security design taking into account system security requirements and resource constraints. Evaluation to obtain the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, partially observable Markov decision process (POMDP) multi-armed bandit problem was formulated. Structural results method to solve the problem for a large network with a variety of nodes was presented. The structural results were easy to implement in practical MANETS and also using the centralized node.

W. Lou, W. Liu et al [4] designed a new security protocol which was used for reliable data delivery to increase the data confidentially service in MANET. A secret message was sent through an insecure medium through a single path; then the enemy could easily compromise by any one of its node. The secret message was divided into multiple pieces via multiple independent paths using secret sharing schemes. In this a whole secret message was not compromised. SPRED could provide secure data transmission in an insecure network.

In [5], R. Yu, H. Tang et al collected the key update of the nodes by their parents or a threshold of sibling nodes acting as a private key generator. The node security in MANETs could change dynamically. Due to that stochastic problem arose in the node selection process; nodes might be safe or some nodes were under attack; a node under attack with private key generator created serious risk in the network. So, when constructing private key generator (PKG) the security states of the node and its energy level of the node were taken into account. From this the best node was selected. This scheme was useful in military field, increasing security and maximized the network life time.

Jay dip Sen. [6] proposed a trust distribution scheme to detect the malicious packet dropping attacks in MANETs. The packet forwarding in the network was dependent on the reputation of the nodes. The reputation information was collected; it stored and exchanged between the nodes, and computed under different scenario. The Reputation Handling Module was used in the trust manager. In the network, each node in the

network independently monitored the behavior of its Neighbors and computes the reputation value for each of its neighboring nodes and next nodes. Simulation result showed the malicious nodes in MANET.

S. Marti [7] proposed a technique that could improve throughput in an ad-hoc network in the presence of nodes that agreed to forward but failed to do so. Ad-hoc network maximized the throughput by using all nodes for routing and forwarding. A node might misbehave by agreeing to forward packets and then fail to do so, because of its being overloaded, selfish, malicious or broken. Two extensions were in the dynamic source routing algorithm (DSR) to detect the misbehaving nodes. Watchdog and pathrater: The watchdog identified misbehaving nodes; the pathrater avoided routing packets through the nodes.

Zhexiong Wei, Helen Tang et al [8] proposed a trust model as trust from direct observation and the trust from indirect observation. With direct observation from the observer node the trust value was derived using an uncertain reasoning, in indirect observation, the trust value was derived from the neighborhood nodes of the observer, the value was derived using Dempster-Shafer theory. The malicious node was detected by the trust value. This scheme differentiated data packets and control packets but dropping of packets due to buffer overflow. Throughput and packet delivery ratio was improved as well as slightly increased delay and overhead.

Kartheesan .L, S.K. Srivatsa [9] said about packet forwarding scheme - trust based scheme for data security mainly on integrity and authentication. Security was provided not only to the data but also for routing information. The trust indexes of the nodes were calculated and the route was selected according to the trust value thus improving integrity. In order to provide authentication, a distributed certificate authority (DCA) technique was required to construct a certificate. Finally the desired level of security was provided by the system based on the user by executing the corresponding security modules. This scheme provided complete production of data in MANET.

Tanapat Anusas-amornkul [10] said that detection and isolation of malicious node was based on cooperative participation of nodes involved in communication based on TRUST level of the nodes. Network performance matrices such as:

a. Delay in Delivery of the Packet
b. Response Time
c. Quality of Service Provider
d. Packet Forwarding Misbehavior

Trust and confidence level computation of nodes in MANET was a challenging task. Untrusted node wreaked PDA more and thus performance degraded abruptly. Trustable node gave more confidence to the network. The respective results were compared with two existing systems and analyzed. It didn't analyze the collaborative malicious packet dropping attack and battery power consumption. Moreover, conditions of "No response" were not analyzed.

Vemana Chary. D, Padmanabham et al [11] introduced a new trust based algorithm to detect colluding nodes because MANETs might have colluding nodes in the network, causing internal attack in the wireless network. Due to this, MANET performance went down and the network broke down. Clustering involved in this

scheme enabled trust computation, route detection and forward node selection process ensured energy efficient routing took place.

Manoj V, Mohammed Aaqib et al [12] proposed the concept of trust and certification authority to fight the misbehaving nodes. Certificate authority employed fuzzy based analyzer to differentiate between trusted and misbehaving nodes. The certificate was distributed only to the trusted node and thus detected the misbehaving node. This was more secure, reliable and improves security in Military operation.

Tarun Kumar Mishra et al proposed [13] a MANET security scheme which reduced overhead based on digital signature. Routing protocols were affected by attacks and presence of compromise nodes. By using the mutual trust between the nodes, attack issue could be solved. Digital signature was used to provide mutual trust between nodes. AODV on demand routing protocol increased performance and reduced routing overhead.

In [14] Flooding attack was one of the types of denial of service type of attacks. Flooding attack sent useless packet in the malicious node. This flooding attack was present in most of the on demand routing protocol, DSR on demand routing protocol using trust estimation function to less serious effect of RREQ flooding attack

F. R. Yu, H. Tang, S. Bu, et al [15] proposed a method to enhance data security using trust based multi-path routing protocol. It discovered a secure destination with less overhead. Misbehaving nodes were detected and removed from that path using the trust value of the nodes. The data were transmitted through multiple paths, increased the robustness because it was almost impossible to reconstruct the original message, the probability was low. Without the use of cryptographic keys the source and destination transmission was secured.

N. Radhika et al [16] proposed a trust model based on, AODV protocol which was an on demand distance vector routing. Rather than performing a digital signature or cryptographic system the proposed model could do trusted route discovery for every packet. Therefore computation overhead could be reduced as well as throughput performance also increased.

Chengyong et al [17] proposed a trusted dynamic source routing protocol which was the extension of widely used DSR protocol and applied the idea of trust concept to prevent from routing misbehavior. Although trust consisted of direct and indirect trust to provide score for the trusted node and therefore routing decision relied on the observed, experienced and forwarding behavior of the other nodes. This scheme increased the efficiency.

S. Buchegger et al [18] proposed a CONFIDENT protocol aimed to detect a malicious node in the network. Important component in that protocol were reputation system, monitor, trust manager and path manager. A node forwarded each packets, the monitor on that node was aimed at confirming that the next-hop node forwarded the packet. When entrusted node was detected on the monitor, reputation system was triggered and it maintained a local rating list. Trust manager handled inputs of other nodes. Finally path manager selected the node route from local rating list and blacklist. In confident protocol scalability problem arose with a number of nodes.

Yan Lindsay et al [19] proposed a trust model based on information theory for improving the security of ad-hoc routing protocol. Similar to other models they

monitor other nodes and exchange recommendations with other nodes in a distributed manner for establishing trust relationship. They fail to render feedback about the decision of security models such as key management mechanism.

Sachin kumar Gupta and R.K Sake [20] evaluated the performance of AODV and DSDV protocol in terms of throughput, the average end to end delay, jitter and drop AODV protocol delivered 70% to 90% of the packet in all cases while DSDV delivered only 50% to 75%.In AODV delay is low after a certain time limit but in DSDV it increased gradually. Finally, the author concluded that AODV protocol is better than DSDV protocol. AODV is suited for real time application in MANETs.

G.Jose moses et al [21] evaluated the performance of AODV, DSR, DSDV based on their performance. The simulation was done on the ns-2 simulator. AODV and DSR performed well when compared to DSDV.

Conclusion

This paper discuss about several trust based method to increasing security in MANET. Trust method detects the malicious nodes. So, that the performance of the network is increased. Trust based mechanism would be better for securing MANET. Choosing an efficient trust model along with a secure routing protocol would increase the security in such networks .And thus this is a never ending research area.

Referance

[1] F. R. Yu, H. Tang, S. Bu, and D. Zheng, “Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks,” EURASIP Wireless Communication. Networking, vol. 2013, pp. 188–190, July 2013

[2] Q.Guan, F. R. Yu, S. Jiang, and V. Leung, “Joint topology control and authentication design in mobile ad hoc networks with cooperative communications,” IEEE Trans. Veh. Tech., vol. 61, pp. 2674 –2685, July 2012

[3] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks,” IEEE Trans. Wireless Communication., vol. 10, pp. 3064 –3073, Sept. 2011.

[4] W. Lou, W. Liu, Y. Zhang, and Y. Fang, “SPREAD: improving network security by multipath routing in mobile ad hoc networks,” ACM Wireless Networks, vol. 15, no. 3, pp. 279–294, Mar. 2009

[5] F. R. Yu, H. Tang, P. Mason, and F. Wang, “A hierarchical identity based key management scheme in tactical mobile ad hoc networks” IEEE Trans. on Network and Service Management, vol. 7, pp. 258 – 267, Dec. 2010.

[6] Jay dip Sen. , “A distributed trust management framework for detecting malicious packet dropping nodes in mobile ad-hoc network” International journal of network security& its application(UNSA),vol.2,no.4.Oct 2010.

[7] S.Marti, T. Giuli K. Lai, and M. Maker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom'00, (New York, NY, USA), Aug. 2000.

[8] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason "Security enhancement for mobile ad-hoc network with trust management using uncertain reasoning" Citation information: DOI 10.1109/TVT.2014.2313865, IEEE Transactions on Vehicular Technology

[9] Kartheesan .L, S.K. Srivatsa" Trust based packet forwarding scheme for data security in mobile ad-hoc network" IOSR Journal of computer engineering (IOSSRJCE) ISSN: 2278-0661vol 2, issue 3(July-August.2012), pp 40-48.

[10] Tanapat Anusas-amornkul, "On detection mechanisms and their performance for packet dropping attack in ad hoc networks", Submitted to the Graduate Faculty of the School of Information Sciences in partial fulfillment of the requirements for the degree of Doctor of Faculty of the School of Information Sciences in partial fulfillment of the requirements for the degree of Doctor of Attack in Ad Hoc Networks",

[11] Vemana Chary. D, Padmanabham. P, Prabhakara Rao. B, **"**Energy efficient routing protocol for Manet using trust based security"**,** International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012.

[12] Manoj V, Mohammed Aaqib , Raghavendiran N and Vijayan R ,"A novel security frame work using trust and fuzzy logic" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[13] Tarun Kumar Mishra, Bhupendra Singh, Arun Kumar, "A security scheme for mobile ad-Hoc networks With reduced routing overhead "International journal of advanced research in computer science and software engineering vol 3,issue 8,August 2013.

[14] Shishir K.Shandilya, Sumita Sahu,"A trust Based security scheme for RREQ flooding attack in Manet" International journal of computer application (0975-8887) vol.5, no.12, August 2010.

[15] F. R. Yu, H. Tang, S. Bu, and D. Zheng, KumKum Garg, and Manoj Misra, "A trust based multi- path routing for enhancing data security in manets" International journal of network security, vol.16, no.2, pp.102-111, Mar.2014.

[16] Dr N.Radhika*, Thejiya V,"Trust based solution for mobile ad-hoc networks" International journal of advanced research in computer science and software engineering, volume 4, issue 5, May 2014 .

[17] Chen Young, Huang Chuanhe, Shi Wenming"Trusted dynamic source routing protocol"Sch.of comput.,WuhanUniv.,WuhanDOI:10.1109/WICOM.2007.411conference: Wireless communication, networking and mobile computing,2007.wicom 2007.International conference on 21-25 September 2007.

[18] S.Buchegger and J.-Y. LeBoudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-

hoc Networks), ” In Proceedings of the 3rd ACM International Symposium on Mobile and Ad Hoc Networking & Computing (MobiHoc 2002), pp. 226–236, Lausanne, Switzerland, June2012.

[19] S.Yan Lindsay, Y. Wei, H. Zhu and K. J. R. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks ”IEEE Journal on Selected Areas in Communications, 24(2), pp. 305-317, 2006.

[20] Jose Moses*, D.SunilKumar, Prof.P.Suresh Varma,N.Supriya,”A simulation based study of AODV,DSR,DSDV routing protocol in MANET using NS-2” International journal of advanced research in computer science and software engineering, volume 2, issue 3, March2012 .

[21] Sachin kumar Gupta*& R.K.Saket “Performance metric comparison of AODV and DSDV routing protocol in MANET susing NS2” www.arpapress.com/volumes/vol7/IJRRAS_7_3_15, June 2011.