Survey on Distributed Trust Management Schemes for Preventing Malicious Activities in Mobile Ad Hoc Network

A.Abitha[1], L. Magthelin Therase[2]
[1]*M.E Embedded System, Sathyabama University, Chennai.*
[2]*Assistant professor, Sathyabama University, Chennai*

Abstract

The open air medium and dynamic nature of MANET suffering from various security demands and globally trust management scheme that enhance security in MANETs. The two methods of trust management are the direct observation and the indirect observation by using uncertain reasoning. In this paper, we are going to extend the energy awareness of the nodes which are participating in the network and introduced originating message confirmation from destination node in a route request manner. When source select the route, source will generate one originating message to all neighbours. Neighbour nodes will check the nearby nodes trust value and that value send to destination. Finally, the result shown in the stimulation is destination analyzes all trust patterns of the routes. Then it will be selects the route without hackers.

Keyword*: Trust management, REQ-accommodation, MANET, OLSR, trust pattern, Trust.*

I. INTRODUCTION

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) have become popular as a key communication technology in military environments. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission, lack of centralized infrastructure of security protection. Classes of approaches that can the safeguard tactical MANETs in the two methods: prevention-based and detection-based approaches. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed. not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals. Then, the infrastructure is destroyed, then the

Whole network paralyzed. Prevention-based approaches can prevent and there are still chances to remain for malicious nodes to participate in the routing procedure and disturb proper routing. In the exiting system the source send the acknowledgement to the destination the attacker will hack the information and send the fake result to the destination. So, the sources only search the hacker, but in this project, the source and destination checks the neighboring of the nodes, whether the attacker is or not. The goal of the project is easily analyses the routes and selects those routes without any hackers.

A. Trust Management

The term "Trust Management" identifying it as a separate component of network security services. In the MANETs in trust management is required for when participating nodes, without earlier interactions, start a network with trust relationships among themselves Trust computations in MANET are challenging because of different types of mobility such as low mobility or high mobility.

B. Trust

Trust concept is important for communication and network protocol designers when creating trust relationships between participating nodes. Trust is not static, it's a dynamic. Trust is subjective. Trust is not transitive. If X trusts Y and Y trusts Z it does not mean that X trusts Z. Trust is asymmetric and cannot be assumed to be reciprocal. In this paper, trust routes and trust pattern to be used.

C. MANET

A Mobile Ad-hoc network is used to information to be exchanged. And the data is forwarding to one node to another nodes and ti cant on the fixed infrastructure. Both host and a router in a node is autonomous terminal. In the distributed operations has no fixed network control and operational management.

One or more nodes that deliver the packet is multi hop routing. In the dynamic neteork topology are form their own network.

Mobile Ad-Hoc network is the infra structure less and also it the self configurable. MANET is On Demand network.

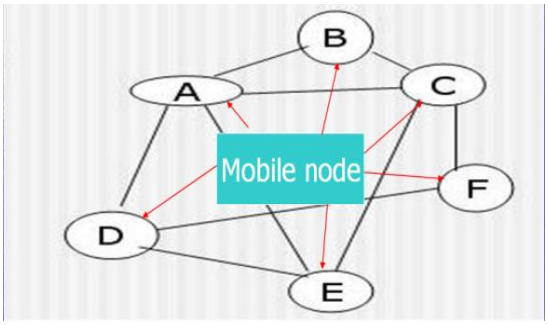

Fig 1 MANET

Problems In MANET

- Routing
- Security and Reliability
- Quality of Service
- Internetworking
- Power Consumption

II. LITERATURE SERVEY

A. Security And Quality Of Service (Qos) Co-Design In Cooperative Mobile Ad Hoc Networks

Qos can be improved by cooperative communication in mobile adhoc Network (MANETs).Idea behind is single-antenna mobile nodes in a Multi user Scenario can share their antennas in a manner that creates a virtual multiple-input and multiple-output (MIMO) system. In the game-theoretic approach to quantitatively analyze the attack strategies of the attacker so as to make a rational decision on relay selection and the authentication parameter adaptation to reach a trade-off between security and QoS in CO-MANETs.

B. Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks

Continuous user authentication is an important prevention-based approach to protect high security mobile adhoc networks (MANETs). On the other hand, to reduce the malicious activities using the intrusion detection systems (IDSs) are also important in MANETs to effectively. Consider these two approaches jointly is 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 is formulated. We present structural results method to solve the problem for a large network with a variety of nodes. The structural results are easy to implement in practical MANETs and also using the centralised nodes.

C. Trust based clustering and secure routing scheme for Mobile Ad hoc Networks

The ad hoc network use the distributed self organizing method and it has uses the security purposes. In the trust evaluation schemes use the fuzzy language in the value of zero and one. The theory of Dempster-Shafe used in order to combine the evidences collected by a cluster head itself and the recommendations from other neighbor nodes. It do not restrict to a single gateway node for inter cluster routing. Cluster ad hoc work based on the secure clustering, secure routing, handing reputation and trust management. So many protocols are used to develop a distributed trust based framework for securing ad hoc networks and to devise a prediction scheme to evaluate degree of trust of each mobile node. It combines the quantifying trust in different matrices and the use of DS theory in order to predict the trust of mobile node more accurately the network.

D. Quantifying Trust in Mobile Ad-hoc Networks

. In the mobile ad hoc network are introduce the A Trust-Domain based security architecture and self-organizing trust-based Physical-Logical Domains. Calculating some equation under the trust formulation and trust evaluation are between pairs of nodes that have been one-hop neighbors at some point of time. and trust model and trust domains described the nodes into trust-based clusters called Physical- Logical Trust Domains. In the solution of the concept is pair-wise trust between two nodes in an ad-hoc network.

E. A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks

In the trust certificate authorities, there is a no online access so is uses a decentralized certificate revocation scheme that allows the nodes within a MANET to revoke the certificates of malicious entities. Base o the cryptographic method it is preventing the malicious nodes and each nodes having the one valid certificate. All key management tasks are except the issuing of certificates, to the selected nodes in a MANET and it does not want any access to on-line certificate authorities (CAs).this certificate revocation scheme is based on weighted accusations and it mainly used as the data origin. Thus the simulation results indicate that when malicious nodes are identified, their certificates are speed in such a way that the nodes in the network are cognizant of the certificates revocation information in a timely manner.

F. A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks

In the trust distribution is used to detecting malicious packet dropping attacks in MANETs. The packet forwarding in the network depends on the reputation of the nodes.. The reputation information is collected; it stored and exchanged between the

nodes, and computed under different scenario. The Reputation Handling Module is used in the trust manager. In the network, each node in the network independently monitors the behavior of its Neighbors and computes the reputation value for each of its neighboring nodes and next nodes. Simulation result that shows the malicious nodes in MANET. Designing an efficient routing algorithm on top of this selfish node detection algorithm.

G. An Efficient and Secure Intrusion Detection Method in Mobile Adhoc Network using Intuitionistic Fuzzy

In the mobile adhoc, to detect the attack by using Intrusion detection system that uses Intuitionistic fuzzy logic which aims to detect distrust behavior of node and identify the attacks if it seems to be an attack based on the MANET and IDS. When implementing this method RREQ based on the Black hole. In the gray hole drops the packet selectively. And, finally the result to be designed the Creating Black hole attack and Creating two different types of gray hole attack.

H. NAODV- Distributed Packet Dropping Attack Detection in MANETs

Detection and isolation of malicious node is 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 is a challenging task. Untrusted node wreaks PDA more and thus performance degrades abruptly. Trustable node gives more Confidence to the network. In the experimented way in various networks settings with various parameters. The respective results are compared with two existing systems and analyzed. It doesn't analyses the collaborative malicious packet dropping attack and battery power consumption. Moreover, conditions of "No response" are not analyzed.

I. Enhancing the Secure Data Transmission for Routing Attacks in MANET

In the Mobile Ad hoc is always used to avoid the routing attacks. When transmitting the data over the network the full file spitted into different packets. Attackers could not only prevent existing paths from being used and choose the non existing paths. And mainly this method used to secure the data transmission against the routing attacks. Dumpster-Shafer theory of evidence with notion of importance factor. These main approach to identify the routing attacks as well as finding attacked node while transmitting data. The table recovery and packet marking data to be sent in less time and secured way.

J. Reasoning about Trust Groups to Coordinate Mobile Ad-Hoc Systems.

In the trust, those to a coordination model have to exploits trust groups in order to establish the safe interactions in the ubiquitous environment. Trust groups are asymmetric, long-lived, lifetime spans an extended period. The dynamics of trust group creation, based on the history of interactions of the device. It represents the Trust information is gathered, in the form of aggregated trust tuples, via a trust management framework. This flat, unorganized information is then processed
to identity fairly stable communities of an agent's most trusted interacting peers, thus actually achieving more efficient and effective coordination.

III. CONCLUSION

In the mobile ad hoc network, detecting the nodes in one direction, by chance it cannot fulfill to reduce the attacker. In this paper, distributed trust management using to prevent malicious nodes by using modified OLSR algorithm. And both the source and destination checks the correct routes without hackers. Data could not be loss; efficiency performance should be good and highly security.

REFERENCES

[1] Pushpita Chatterjee School of Information Technology Trust Based Clustering And Secure Routing Scheme For Mobile Ad Hoc Networks International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, July 2009.

[2] Mohit Virendra, Murtuza Jadliwala, Madhusudhanan Chandrasekaran, Shambhu Upadhyaya Quantifying Trust in Mobile Ad-Hoc Networks KIMAS 2005 WALTHAM, MA, USA

[3] L. Eschenauer, V.D. Gligor, "A key-management scheme for distributed sensor networks", *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pp. 41-47, Washington D.C., 2002

[4] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks*", Proceedings of 9th International Conference on Network Protocols (ICNP '01)*, pp. 251-260, 2001

[5] Bucheggar, S., Boudec, J.Y.: Performance analysis of the CONFIDANT Protocol: Cooperation of Nodes-Fairness in Dynamic Ad Hoc Networks'. In: Proceedings of the 3rd Symposium Mobile Ad-Hoc Networking and Computing, pp. 226-236 (2000).

[6] Azzedin, F. and Maheswaran, M.: Evolving and Managing Trust in Grid Computing Systems. In: Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (2002).

[7] Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust Cooperative Trust Establishment for MANETs," *Proc. 4th ACM Workshop on Security of Ad Hoc and Sensor* Networks, Alexandria, VA, 30 Oct. 2006, pp. 23-34

[8] L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," *Proc. 2nd UK-UbiNet Workshop*, 5-7 May 2004, Cambridge University, Cambridge, UK

[9] W. J. Adams, N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration,"

Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW'05), 15-17 June, 2005, West Point, NY, pp. 317-324.

[10] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," *Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks*, Baltimore, MD, Aug. – 1 Sep. 2006, pp. 1-7.

[11] 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 Philosophy University of Pittsburgh 2008.

[12] Shukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in
Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science 2008, USA.

[13] [12] X. Li, X. Wang, and J. Shen, "Strategy and simulation of trust cluster based key management protocol for ad hoc networks," *4th Int'l Conf. on Computer Science & Education*, pp. 269 - 274, Nanning, China, July 2009.