International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Literature Review of Enhancing Security in Mobile Ad-Hoc Networks Using Trust Management Security Scheme

Rajshree Ambatkar[1], Purnima Selokar[2]

[1]Department of C.S.E, G. H. Raisoni institute of Engineering and Technology for Women, Nagpur University, Nagpur, India

[2]Department of W.C.C, G. H. Raisoni institute of Engineering and Technology for Women, Nagpur University, Nagpur, India

Abstract: ***A mobile ad hoc network (MANET) is formed with wireless mobile devices (nodes) without the need for existing network infrastructure. Security design in MANET (Mobile advoc network) is complicated because of its features including lack of infrastructure, mobility of nodes; dynamic topology and open wireless medium .Due to this MANET suffer from many security vulnerability. To enhance the security, it is very important to rate the other node which is trustworthy. Hence a unified trust management security scheme is used. In trust management security scheme, the trust model has two components: direct observation and indirect observation. In direct observation, trust value is calculated from an observer node to observed node. On the other hand, indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node; the trust value is calculated between them. By combining these two components in the trust model, a more accurate trust value is obtained. This will help to improve throughput and packet delivery ratio in the network.***

Keywords: MANETs, Security, Trust Management, uncertain reasoning.

1. Roduction

A MANET Stands for "Mobile Ad Hoc Network." is a type of ad hoc network that can dynamically change locations and self configuring on the fly. Because MANET consist of mobile nodes, they use wireless connections to connect directly or relying on other mobile node as router to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission [1][9]. In cases, where no network infrastructure exists, such as in war zones, relief efforts in remote territories, and emergency situations a mobile ad hoc network is used. Such network does not depend on preexisting/centralized infrastructure and base stations. In decentralized network all network activity including discovering the topology and delivering messages to the other nodes must be executed by the nodes themselves [2]. The applications for MANETs are diverse, ranging from small, static networks to large-scale mobile highly dynamic networks [1]. Other than application, MANETs need efficient distributed algorithms to determine network organization, link scheduling and routing [2] [7]. The network protocol which is design for these networks is such a complex issue [2].

Open and closed are the two types of MANETs [1].In open MANET, different nodes having different goals and they share their resources with each other for connecting globally. In closed MANET, all mobile nodes which are in networks cooperate with each other to achieve a common goal. MANET suffers from many security attacks Because of its distinct features including lack of infrastructure, node mobility, dynamic topology and open wireless medium [5]. Therefore security is challenging issue in MANET [1]: Cryptography and key management schemes seem good [5], but they are too expensive in MANET. Prevention-based and detection based are the two approaches that are used in MANET [6]. IN prevention-based approaches a centralized key management is required, which may not be possible in MANET because of its distributed networks. The whole network may be affected if the infrastructure is destroyed. So this approach is used to prevent misbehavior but not detect malicious nodes. Detection based approaches are used to detect selfish node that helps to identify **malicious misbehavior. Detection based approaches are based on trust in MANETs [3]. Hence this approach is used to** calculate trust value in trust management schemes.

Most of the detection based approaches based on trust in MANETs, may not use both direct and indirect observation (second hand information obtained from neighbor node or third party node) .Trust evaluated from direct observation not able to differentiate data and control packets. For security in MANETs, it is important to identify nodes that are trustworthy to other nodes without using centralized authorities for building up a trust environment. Such mechanisms not only help to detect malicious node, but also improve network performance. For evaluating trust value we are using both direct & indirect observation. In this paper, trust value calculation means degree of belief that is node performs as expected. Hence, unified trust management security scheme is used to enhance security of MANET

2. Literature Review

- In paper “Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning” [1] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang & Peter Mason, IEEE transaction paper2014 has discussed that because of Dynamic topology & open wireless medium MANETs suffering from many security vulnerabilities. Hence a Unified trust management scheme is used to enhance the security in MANETs. In this scheme, the trust model has divided into components:

Trust value is calculated from direct and indirect observation.

- In paper "A Survey of Secure Mobile Ad Hoc Routing Protocols"[2] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani,IEEE transaction paper 1999 has discussed that Several routing protocols have been used in Mobile Ad hoc Networks (MANETs) such as military, government & commercial applications. These protocols focus on security issues and differentiate in terms of routing methodologies. Four routing protocols are most widely used for analysis and evaluation including: AODV, DSR, OLSR and TORA.
- In paper "Joint topology control and authentication design in MANET with cooperative communication, [3] Q.Guan, F.R.Yu, S.Jiang IEEE Transaction paper 2012 has discussed that Mobile ad hoc networks (MANETs) based on cooperative communication (CC) suffering from many challenges regarding security, network performance & management issues. Joint authentication & topology control (JATC) scheme is used that combine both Authentication & topology control to improve the throughput.
- In paper "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" [4] Kejun Liu, Jing Deng, pramod K. Varshney, Kashyap Balakrishnan, IEEE transaction paper 2011 has discussed that routing misbehavior can be avoid using acknowledgement scheme. 2ACK scheme is used to detect misbehavior in routing and mitigate their effect.
- In paper "Securing Mobile Ad Hoc Networks with Certificate less Public Keys"[5] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, IEEE Transaction 2006 has discussed that a fundamental problem in securing MANETs. IKM is an ID-based key management scheme which is a combination of ID-based & threshold cryptography. IKM is a certificateless solution that eliminates need for certificate-based authenticated public-key distribution
- In paper "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks" [7] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, and Helen Tang, IEEE Transaction 2011 has discussed that how effectively malicious activities can be identified. Intrusion detection systems (IDSs) and user authentication these two approaches jointly consider for effective security design.

3. Proposed Methodology

The main goal of MANET is to establish trusted connection amongst each other. In detection based approaches, Unified trust management security scheme is one of the important methods [1]. By using trust information, node does not take highly risky action such as forwarding or sending the data packet to the node which is having low trust value. In trust management security scheme, trust model has two components: trust value which is calculated from direct observation & indirect observation. In direct observation, trust value is calculated from an observer node to observed node. Indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node. Indirect observation or second-hand information is used to evaluate trust value of observed nodes from neighbor node. Indirect information is very important as Compared to direct observation. Example: information collected from neighbor nodes can able to detect situation where particular node's behavioral is well or not.

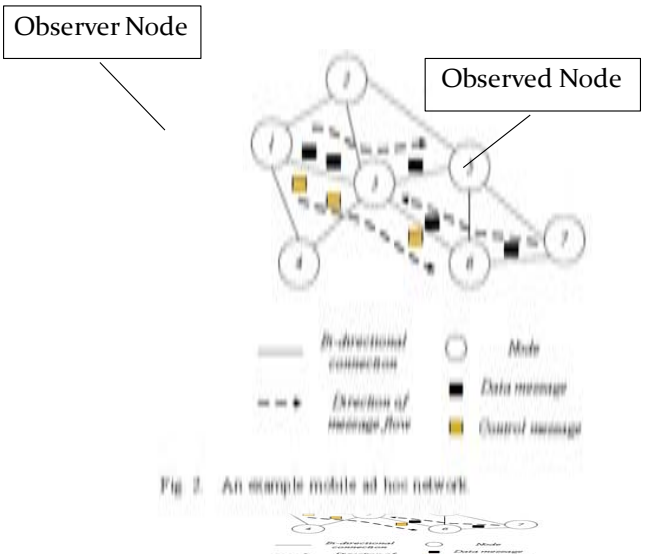

Figure 1:.An example Mobile Ad hoc network

In this example, two types of messages send between nodes data and control messages. Node 1 is act as an observer node and node 3 is an observed node. In this case Node 1 sends data messages through node 3 to node 5. When node 3 forwards messages to node 5 then node 1 can observe the communication this is direct observation. Based on this observation node 1 can calculate the trust value of node 3. The same idea is applied to the control message situation. Meanwhile, node 1 can collect information from node 2 and node 4 to evaluate the trust value of node 3.Here node 2 and node 4 are neighbor nodes of node1 and information collected from third party nodes is called indirection observation.

4. Techniques Used To Identify Selfish Nodes

Selfish or misbehaving nodes which are present in MANET can disrupt the working of network and degrade the performance of the network. Hence, it is very important to detect and remove these selfish nodes. Following are the various techniques available to prevent the selfishness in MANETs [4]:

a) Cooperative Communications

Using cooperating mediator nodes in the network, Mobile devices in ad hoc networks communicate with each other through a multi-hop route. Cooperative communication between nodes has been important to improve transmission reliability, performance and security of the network. If centralize coordination is not present between nodes, then many security issues may arrives. For example if selfish node present in network, then nodes does not cooperate with each other and start dropping packets. In MANET battery power is considered to be more important hence to reduce battery power consumption, nodes refuse to share its own resources and such nodes are selfish node. Selfish node may participate in the route discovery and maintenance process but they rejected to forward data packets. So

because of these malicious node packet delivery ratios deteriorate or break significantly.

b) Credit Based System

In credit-based schemes, the basic idea is to provide incentives for the nodes that sincerely perform their task. Virtual (electronic) currency or similar payment system may be used to perform networking functions such as forwarding and receiving packets. Payment is given to the nodes for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services [4]. Several schemes are used credit based system for packet forwarding: Packet Purse Model and the Packet Trade Model. Another scheme is Sprite, in which nodes keep receipts of the received/forwarded messages. The main problem with credit-based schemes is that tamper-resistant hardware and/or extra protection for the virtual currency is required in this scheme.

c) Reputation-based scheme

Reputation or trust based models are one of the approaches that enforce cooperation between nodes and mitigate node misbehavior. Reputation is a factor which is calculated through direct interactions through monitoring or observing the nodes and/or indirect information collected from neighbors. A node can trust its direct information more than the indirect information. Reputation based schemes are classified based on their monitoring component: as using either active or passive acknowledgments.

Example of Reputation-based scheme:-

- *Watchdog*: Watchdog technique is used to detect routing misbehavior and mitigate its effect in MANETs. In watchdog technique, it observer the medium to check whether the next hop node is trustworthy and maintains the buffer to store recently sent packets. If a data packet present in the buffer for long time, the watchdog module accuses next-hop neighbor misbehavior.
- *Pathrater:* Based on the watchdog's allegation, the pathrater module give rating to every path in its cache and subsequently chooses the best paths that avoid nodes misbehavior. This technique is more reliable than watchdog technique.
- *Confidant:* Cooperation of Nodes-Fairness in Dynamic Ad-hoc Networks (CONFIDANT) is a security model for MANETs based on selective altruism and utilitarianism [6]. In this scheme, for computation of reputation values both first-hand and second-hand information is used. It is a distributed, symmetric reputation model most commonly used.

5. Conclusion

A unified trust management security scheme is used to enhance the security of MANETs. Using recent advances in 'Uncertain Reasoning', system evaluates the trust values of observed nodes in MANETs. In MANET Misbehavior such as 'Dropping' or 'Modifying packets', can be detected through trust values which is obtained by direct and indirect observation and Nodes with low trust values will be excluded or remove by the routing algorithm. In this way secure routing path can be established in malicious environments which help to improves throughput and packet delivery ratio.

References

[1] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE transaction paper 2014.
[2] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE transaction paper 1999
[3] 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.
[4] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transaction paper 2011
[5] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable and Secure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.
[6] Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks,"IEEE Trans. Veh. Tech., vol. 60, pp. 1025–1036, Mar. 2011.
[7] 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 Commun., vol. 10,pp. 3064 –3073, Sept. 2011.