RESEARCH ARTICLE OPEN ACCESS

Increasing the Quality of Security of Mobile Ad-Hoc Networks

Sharmila Chopade, Mohini Mohite, Bhagyashri Narwade, Mahadevi Barche
Computer Department
Pune University, DYPIET Ambi
India

ABSTRACT

Security enhancement have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to co-ordinate military deployment among the soldiers, vehicles and operational command centers. Military environments has many risks needed to be considered seriously due to the clear features of MANETs, including open wireless link, lack of centralized infrastructure of security protection. Security Trust Management Scheme and Trust Identity Acknowledgment (TIA) are the two solutions for the risk. Direct observation and indirect observation are two components of trust management scheme. The trust value is calculated using Bayesian inference in direct observation and the trusts value is calculated using the Dempster -Shafer Theory (DST) in indirect observation. The throughput and Packet Delivery Ratio (PDR) of observed node is improved and security is maintained and enhanced.

Keywords:- *MANET-Mobile Ad Hoc Network, Security Trust Management (STM), Trust Identity Acknowledgement (TIA), Dempster-Shafer Theory (DST), Security Enhancement (SE).*

I. INTRODUCTION

MANET is the collection of nodes that connect with each other with the help of wireless link. Nodes are moved from one place to another place in topology. Node is co-operating with each other and route the packets. Trust on the node and managing nodes are the major issues in MANET because of having the less resource and process complexity. MANET is a challenging research factor because of security. The two complementary classes of approaches of MANETs, one is prevention-based approach and second is detection based approach. A centralized key management infrastructure is one of the issue of the Prevention based approach, which may not be realistic in MANETs such as distributed networks. Prevention based approaches can prevent misbehavior. Detection based approaches can identify malicious activities based on trust. Some excellent work has been done on detection based approaches in MANETs. Detection based approaches do not support direct and indirect observation at the same time to evaluate the trust of an observed node. Indirect observation is used to access the reliability of nodes. Data packets and control packets are do not differentiate by trust methods. Detection of packet drop uses TWOACK, S-ACK, AACK acknowledgement schemes to overcome the defects. TWOACK method is used to detect misbehaving link by acknowledging data packets transmitted over each nodes along with the path from source to destination. MANETs control packets usually are more important than data packets. MANET interprets trust, that a node performs as expected. MANET proposes a trust management scheme to increase the quality of the security of MANETs with the help of interpretation.

II. MOTIVATION

MANET propose, security management schemes that enhances the security of MANET. The Bayesian inferences DST protocol used to calculate the trust value of observed node in the MANET'S. The malicious activity, missing packets or modifying packets can be detected through the trust value. Trust value can be calculated by the trust direct and indirect value.

III. LITERATURE SURVEY

A. Securing mobile ad hoc networks with certificate less public keys (CPK) [3]: As the future research, intend to determine the efficiency of the proposed schemes through simulations and practical implementations.

B. Survey of Secure Mobile Ad Hoc Routing Protocols [1]: 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. AODV, DSR, OLSR and TORA protocols are most widely used for analysis and evaluation.

C. Mitigating routing misbehavior in mobile ad hoc networks (MRM)[2]: Mitigation would like to evaluate the watchdog and considering latency in addition to throughput.

D. Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks (CCAID) [6]: Malicious activities can be identified. Intrusion detection systems (IDSs) and user authentication these two approaches jointly consider for effective security design. Continuous user authentication is an important prevention-based approach to protect high security mobile ad-hoc networks (MANETs). Intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities.

E. hierarchical identity based key management scheme in tactical mobile ad hoc networks (HTM) [5]: As the future research, directions to develop trust management model with desirable attributes such as adaptation to environmental dynamics, scalability, reliability, and reconfigurability

F. Securing resource-constrained wireless Ad-hoc networks (SRC)[4]: The protocols Should be further optimized and expanded in the future. However, nothing stands in the way of using mesh networks.

G. A mean field game theoretic approach for security enhancements in mobile ad hoc networks Wireless Communication (GTA) [7]: GTA are going to extend trust aware with energy aware AODV protocol. While knowledge forwarding, the nodes can amendment the trail supported energy state of each nodes. Thus GTA able to improve the QOS with improved security. Finally QOS able to improve prolong network.

IV. SYSTEM DESIGN

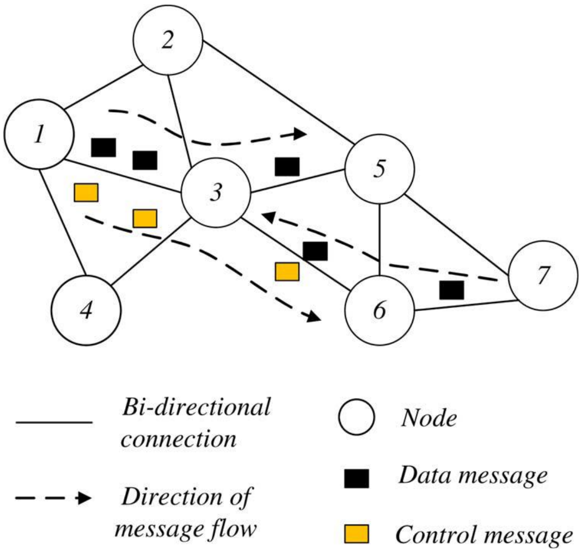

Fig. 1 Example of mobile ad hoc network

To explain the basic procedure of trust evaluation in scenario, an example network is shown in Fig. 1. In this example, node 1 is an observer node, and node 3 is an observed node. Node 1 transmits data through node 3 to node 5. When node 3 receives data messages and forwards to node 5, node 1 can overhear it. Then, node 1 can evaluate the trust value of node 3 based on data messages. The same idea is applied to control message situation. Means, node 1 can obtain information from nodes 2 and 4, which have interactions with node 3 to evaluate the trust value of node 3. This information obtained from third-party nodes is called indirection observation

Table 1: Literature Survey

Sr no	Yea r	Approache s	Advantages	Limitations
1.	1999	Survey of Secure Mobile Ad Hoc Routing Protocols	Dynamic topologies, bandwidth, variable capacity links.	Few works have been done on availability but integrity is not taken in consideration.
2.	2000	Mitigation Routing Misbehavio r	Increase throughput, done without a priori trust.	Mitigation would like to evaluate the watchdog and considering latency in addition to throughput.
3.	2006	Certificate Public Keys	Detecting and removing the malicious nodes in network.	CPK intend to evaluate and justify the efficiency of the proposed schemes.
4.	2009	Securing Resource Constraine d	The protocols should be further optimized and expanded in the future.	Computational complexity of the pairing operations
5.	2010	Tactical	The dynamic	Develop trust

		Mobile	node selection process is formulated.	management model with desirable attributes such as adaptation.
6.	2011	Combined Continuous User Authentication and Intrusion Detection	Effectively identify malicious activity.	Mobility and wireless channels, for making the scheduling decisions in MANET are not considered.
7.	2014	Game Theory Approach	Improve QOS which able to improve prolong network.	Performance with limited energy. .

V. CONCLUSION

The security of mobile ad hoc networks enhanced by using Trust Management Scheme that includes direct and indirect observations. The use of uncertain reasoning will provide finest value for the trust variable. Bayesian inference with direct observation and Dempster Shafer Theory with indirect observation are used to calculate the trust value. Trust assurance using fuzzy logic is another better method. Trust assurance registers each node needed for data transmission and sends the data.

ACKNOWLEDGEMENT

The authors which making their resources available would like to thank the publishers, researchers and teachers for their guidance. We also thank authority of the college for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends and family members.

REFERENCES

[1] S. Corson and J. Macker , Mobile Ad Hoc Networking (MANET): “*Routing protocol performance issues and evaluation considerations”*, Jan. 1999, IETF RFC 2501.

[2] S. Marti, T. Giuli, K. Lai, and M. Maker, “*Mitigating routing misbehavior in mobile ad hoc networks*,” in *Proc. ACM MobiCom*, Aug. 2000, pp. 255–265.

[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “*Securing mobile ad hoc networks with certificateless public keys*,” *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.

[4] Y. Fang, X. Zhu, and Y. Zhang, “*Securing resource-constrained wireless ad hoc networks*,” *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, Apr. 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. Netw. Serv. Manag.*, vol. 7, no. 4, pp. 258–267, Dec. 2010.

[6] S. 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. Technol.*, vol. 60, no. 3, pp. 1025–1036, Mar. 2011.

[7] 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, no. 6, pp. 2674–2685, Jul. 2012.

[8] Y. Wang, F. R. Yu, H. Tang, and M. Huang, “*A mean field game theoretic approach for security enhancements in mobile ad hoc networks*,”*IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627,Mar. 2014.