International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 9 (2013), pp. 909-916
© International Research Publications House
http://www. irphouse.com /ijict.htm

A Novel Technique of Securing Mobile Adhoc Networks using Shared Trust Model

Suyash Bhardwaj[1], Swati Aggarwal[2] and Shikha Goel[3]

[1]Department of Computer Science & Engineering, Faculty of Engineering & Technology, Gurukul Kangri University, Haridwar.
[2]Department of Computer Application, IMS Engineering College, Ghaziabad.
[3]Department of Computer Science & Engineering, RKGIT, Ghaziabad.

Abstract

Mobile Adhoc Networks (MANETs) are mostly used in the conditions where any fixed backbone infrastructure is not available. They are easy to implement but they are more prone to attacks and threats. Being mobile and using distributed services are few of the weak points of security in MANETs. As the communication system keeps on changing during its life span and new communicating nodes keeps on coming and old keeps on moving out of the network. Hence there is need for keeping the record and to provide proper authentication for the new arriving nodes and the existing nodes in the network. But because of intrusion threats and various other kinds of attacks it is difficult to judge any new node and to allow only safe nodes to get connected with the existing safe system. Here in this paper we propose a model for authenticating the new nodes as well the nodes which are active in current communication network on the basis of concept of shared trust. For the initialization of the network the few trusted nodes will be allowed to form a neighbourhood of trusted nodes with their initial entries in a Stationary Secure Database (SSD). Now when the group grow in size these trusted nodes will be communicating with each other and will allow or disallow the trusted or compromised nodes respectively on the basis of shared trusted model to establish a secured, stable, trustworthy group of mobile nodes.

Keywords: MANETs, Stationary Secure Database, Trust computation, Trust Propagation.

1. Introduction

A mobile ad hoc network (MANET) is a self-configuring network that is created by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is able to communicate with other nodes in its communication range with a wireless transmitter and receiver. If a node wants to communicate with other nodes that are out of its coverage area, its need to cooperate with other nodes in between; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. As MANETs become widely used, the security issue has become one of the primary fields of concern.

There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication and many other techniques [1, 2, 3, 4] have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack before it is going to occur, we can stop any malicious node from doing any damage to the system or any data. Here is where the concept of trust based system comes in.

2. Concept of Trust

Trust evaluation is implemented according to normal human psychology and subsequent behaviour. In real world environments, when making decision, people normally trust the person they know personally and/or have known from someone else. They trust them till they are in a good relation with them. So how much trust a person can have on other is a relative term, if he is in communication with the person than it is supposed to be trustworthy otherwise not.

The MANETs are usually architecture independent networks, the work is distributed and the mutual cooperation of all nodes in the network is needed, which is based on the trust that these nodes would act as expected. However, taking each and every node to be trustworthy may not be always true, as some nodes may be compromised and behave selfishly or even maliciously to disrupt the network operation. Employing cryptographic mechanisms can protect the correctness and integrity of the information being transmitted in the system, but these mechanisms cannot answer the question about the trustworthiness of each party and predict their behaviours. By evaluating the trustworthiness of related parties, it is easier to take proper security measures and make proper decision on any security issues.

In this paper, we examine the vulnerabilities of wireless networks and state that we must include trust based mechanisms for securing MANETs. We propose a new trust based model to quantify the trust level of the nodes in MANETs.

3. Design of Trust Model

The use of trust as the factor for design and development of secure systems is a new and upcoming method in the field of MANETs. The trust model security features can be directly applied on the network to reduce the probability of a node for being attacked or being compromised and hence improves routing [5].

A trust model should be able to fit in various scenarios of the system. In an open MANET, nodes may be free to join or leave the network anytime at will. Some nodes may or may not already know each other before they join the network. Besides the direct interaction experience in the network, the pre-shared knowledge, if any, is also quite important for a node to implement trust evaluation and should be taken into account in a trust model.

The application of Stationary Secure Database (SSD) is to give a secure, trusted repository for mobile nodes to obtain information about the latest misuse signatures and to find the latest patterns of normal user activity. The use of the SSD to mine new anomaly rules is beneficial to the IDS for three reasons. First, the SSD will be fixed, so it will be fast and is capable of mining rules much faster than on slower, mobile nodes. Secondly, the processing time used to mine the new rules will not take away from the processing time of the mobile nodes. And thirdly, the SSD is capable of having much more storage capacity to store an abundance of audit data collected from the nodes. It is very likely that the mobile nodes will not have enough storage to store substantial amounts of audit data, but by uploading audit data to the SSD, no data is deleted because of lack of storage space.

4. Literature Review

Extensive work has been carried out in the different aspects of proposing security models in MANETs. The work related to trust can be seen in information technology as, trust metrics and trust evaluation are mainly defined for public key authentication [6,7,8,9,10] access control [11] and electronic commerce[12, 13]. Ngai, Lyu and Chin [14] proposed an authentication service against dishonest nodes in MANET, by applying Beth, Borcherding and Klein's trust evaluation model designed in [15]. In Beth, Borcherding and Klein's approach, two types of trust are measured: direct trust and recommendation trust. Pirzada and McDonald [16, 17] proposed a trust model to establish trust in pure MANETs. The trust computation is based on monitoring data delivery in the network. Yan, Zhang and Virtanen [18] proposed a trust model for secure routing evaluation in MANET. The authors defined a large trust evaluation matrix based on statistic data collected during the network communication. Virendra, et al. [19] proposed a pair-wise trust evaluation scheme in MANETs. Jared Cordasco et al. [20] gave his perspective of Cryptographic Versus Trust-based Methods for MANET Routing Security. In their survey on Trust Computations and Trust Dynamics in Mobile Adhoc Networks, Kannan Govindan & Prasant Mohapatra [21] covered up various issues and challenges in the trust computation and propagation of trust in a hostile environment. Jin-Hee Cho, & Ananthram Swami [22] worked on Trust-based

Cognitive Networks and gave their views on Trust Management for Mobile Ad Hoc Networks.

The above related work discusses the various schemes of trust propagation and trusted networks but they have limitations for sharing or monitoring data delivery. Such approaches are suitable to routing trust evaluation, but not sufficient for node authentication in MANETs.

5. Shared Trust Evaluation Model

In this part we present the details of our trust evaluation model that can be used for node authentication in MANETs. Our trust model could overcome the limitations of current approach addressed above.

Trust is a notation of human behaviour. The basic definition of trust can be given as "Trust is the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context" [23].

5.1 Trust Quantification & Trust Computation

Trust quantification reflects various degrees of trust or distrust that a trustor node may have on a trustee node. In this paper, we express trust quantification with real number between 0 and 1. The more closure to zero represents the more degree of distrust. 1 is the maximum value that represents as absolute trust. The number 0 is a natural trust value for a new or unknown node.

In our model The trust is calculated in two types one is global trust and second is local trust. Global trust Tg is the average of addition of all local trust associated with the nodes

$$Tg = \frac{\sum_1^n Tli}{n} \quad (1)$$

and local trust Tl is the ratio of trust of Wi Weight of experience in trusted communication and Ti time for which it has been ideal.

$$Tl = \frac{Wi}{Wi+Ti} \quad (2)$$

The weight of experience is calculated as the number of successful and trusted communications of the node with other nodes. Initially when a node comes in the network after being checked through a local intrusion detection systems or some security mechanism it will be allowed in the network and hence it will get W_i as 1 at initial time. Now the local trust of the node will decrease fraction by fraction by the time Ti when it is not involved in any type of communication.

5.2 Making Decision

To decide that whether a node is trusted or not for current communication the difference of local trust Tl with the dynamic $Tthreshold$ is taken into account, the decision factor D is defined as

$$D = Tl - Tthreshold \quad (3)$$

If D>=0, it means the computed trust value satisfies the trust requirement of the ongoing task. If D<0, it means that the trust requirement is not satisfied.

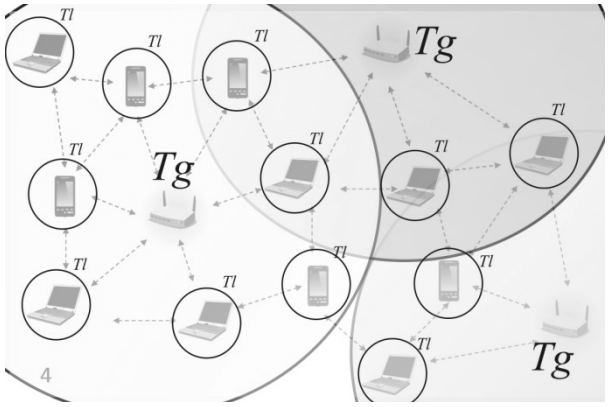

Figure 1: Shared Trust Model.

6. Working of Shared Trust Model

Our model is designed to provide flexible and effective trust evaluation for dynamic MANETs and can be applied for node authentication in open network environment. Whenever a new node arrives in the network it will request the permission to get connected with the network. If it turns safe from intrusion detection system installed at the devices and pass though base level security, then it will be allowed in the network. Later as the time passes its trust level will decrease on its own if it does not communicate with the neighbouring nodes, and its will be soon moved out of the trusted network if the local trust level drops below the threshold.

A case may arise when a malicious node may mislead the trust evaluation by presenting false trust value. To avoid such cases the decision factor uses a global dynamic threshold value for guarantee the node to stay in the communication otherwise leave the network. Once a misbehaving node is detected, such as masquerading as another node or maliciously modifying others public key information through the transmission, the detecting node may send an acknowledge message to other nodes, together with its updated trust value on the misbehaved node as recommendation.

7. Conclusions and Future Work

In this paper, we proposed a new model to enumerate use of trust in establishing secure MANET. Our proposal is distributed, effective and does not depend itself on any central network. In our proposal, both pre-existing knowledge and direct interaction among nodes in the network can be taken into account as a quantity of experience for

their trust evaluation. To quantify the trust value in local and global space, we used new computation function *Tl* and *Tg*, which enables the systems to understand its topology and trust level security. Our proposal deals with the fundamental trust establishment problem and can serve as the building block for higher level security solutions such as key management schemes or secure routing protocols.

References

[1] M. G. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," *ACM Mobile Computing and Communication Review (MC2R)*, Vol. 6, No. 3, pp. 106-107, July 2002.

[2] Y. Hu, D. B. Johnson, and A. Perrig, SEAD: Secure Eficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, pp. 3-13, June 2002.

[3] Y. Hu, A. Perrig, and D. B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02)*, pp. 12-23, September 2002.

[4] Perrig, R. Canetti, D. Tygar and D. Song, \The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, 5 (Summer), 2002.

[5] Dewan, P. and P. Dasgupta. Trusting Routers and Relays in Ad hoc Networks. in Proceed-ings of First International Workshop on Wireless Security and Privacy (WiSr 2003) in con- junction with IEEE 2003 International Conference on Parallel Processing Workshops (ICPP). 2003. Kahosiung, Taiwan: IEEE.

[6] Reiter, M.K. and S.G. Stubblebine, Resilient authentication using path independence. IEEE Transactions on Computers, 1998. v 47(n 12).

[7] Maurer, U., Modelling a Public-Key Infrastructure. Lecture Notes in Computer Science, Springer-Verlag 1996. v 1146: p. 325.

[8] Josang, A. An Algebra for Assessing Trust in Certification Chains. in Proceedings 1999 Network and Distributed System Security Symposium. 1999. Reston, VA, USA: Internet Society.

[9] Levien, R. and A. Aiken. Attack-resistant trust metrics for public key certification. in Proceedings of the Seventh USENIX Security Symposium. 1998. San Antonio, TX, USA: USENIX Association.

[10] Zimmermann, P.R., The Official PGP User's Guide. 1995: MIT Press.

[11] Herzberg, A., Y. Mass, and J. Michaeli. Access control meets public key infrastructure, or: assigning roles to strangers. in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 2000. Berkeley, CA, USA: IEEE.

[12] Manchala, D.W. Trust Metrics, Models and Protocols for Electronic Commerce Transactions. in Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No.98CB36183). 1998. Los Alamitos, CA, USA: IEEE Computer Society.
[13] Manchala, D.W., E-commerce trust metrics and models. IEEE Internet Computing, IEEE 2000. 4(n2): p. p 36-44.
[14] Nagi, E.C.H., M.R. Lyu, and R.T. Chin. An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks. in Proceedings of 2004 IEEE Aerospace Conference. 2004. Big Sky, MT, United States: IEEE.
[15] Beth, T., M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. in 3rd European Symposium on Research in Computer Security (ESORICS '94). 1994. Brighton, UK: Springer Verlag.
[16] Pirzada, A.A. and C. McDonald. Trusted Route Discovery with TORA Protocol. in the Second Annual Conference on Communication Networks and Services Research (CNSR'04). 2004. Fredericton, N.B., Canada: IEEE.
[17] Pirzada, A.A. and C. McDonald. Establishing trust in pure ad-hoc networks. in Proceedings of the 27th conference on Australasian computer science. 2004. Dunedin, New Zealand: Australian Computer Society.
[18] Yan, Z., P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solution in Ad Hoc Networks. in Proceedings of the Seventh Nordic Workshop on Secure IT Systems 2003. 2003. Norway.
[19] Virendra, M., et al. Quantifying Trust in Mobile Ad-Hoc Networks. in International Con-ference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05). 2005. Waltham, Massachusetts, USA: IEEE.
[20] Jared Cordasco, Susanne Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security" Department of Computer Science, Stevens Institute of Technology, Hoboken, New Jersey USA
[21] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey"
[22] Jin-Hee Cho, Ananthram Swami, "Towards Trust-based Cognitive Networks:
[23] A Survey of Trust Management for Mobile Ad Hoc Networks" Army Research Laboratory – Computer and Information Sciences Directorate, 14th ICCRTS, "C2 and Agility".
[24] Grandison, T.W.A., Trust Management for Internet Applications, in Department of Computing. 2003, University of London: London, British. p. 252.