Journal of IMS Group
Vol. 12, No. 1, Jan-June 2015, pp. 66-72

Self-Securing Mobile Ad Hoc Network Using Distributed Trust Model

Suyash Bhardwaj and Swati Aggarwal

Abstract

Mobile Adhoc Networks (MANETs) are easily deployable and infrastructure less networks. Being substantial and adaptable they are mostly used in uneven terrains or war situations. But their use comes in handy in day to day life as well. Being mobile and using distributed services MANETs act as a complimentary service based network for coping with the needs of every type of industry or home networks. As the communication systems have evolved in last few decades, have made the security of the networks a key issue in present scenario. Here in this paper we are going to present a self-securing network model which keeps a track of all the nodes communicating in its neighbourhood of trusted nodes, and when an outsider node arrives in the active network it shall be given a ticket to communicate with the nodes after being checked for impersonation or repudiation attacks. This ticket will expire within given time after a silent gap of not communicating with the active nodes. The benefits of such model is that in case if the node is being compromised it would automatically will be tossed out of the network hence making them self-secure. 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 distributed trust model to establish a secured, stable, trustworthy group of mobile nodes.

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

INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that can be deployed at any place at any time with least prerequisite of 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 communic-

Suyash Bhardwaj
Department of Computer Science and Engineering
Faculty of Engineering and Technology
Gurukul Kangri University
Haridwar, Uttar Pradesh
suyash.bhardwaj@gmail.com

Swati Aggarwal
Department of Computer Application
Gurukul Mahavidhyalaya
Dehradun, Uttar Pradesh
aggarwalswati37@gmail.com

ation. 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 concerns.

Regardless of passive and active attacks in MANETs many Proactive approaches such as cryptography and authentication and many other techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the concept of self-securing networks comes in MANETs .

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

SELF-SECURING AD HOC WIRELESS NETWORKS

Since wireless ad hoc networks are not based on any fixed infrastructure, it is cumbersome to have any third party trusted certification authority in place. However this problem is overcome by distributing the certification on individual member nodes.

The model presented in this paper suggests a mobile IDS based trust model to distribute the function of a trusted third party Certification Authority (CA) to individual member nodes within the network. In the mobile IDS based trust model, a node is trusted if any k (threshold) trusted entities claim so within a certain time period. These certifying entities are generally the nodes one hop neighbours. Once a node is trusted by its local community, it is globally accepted as a trusted node; otherwise it is considered untrustworthy in the entire network. If a node could not find k neighbours in certain location, it may roam to meet more nodes or wait for new nodes to move in.

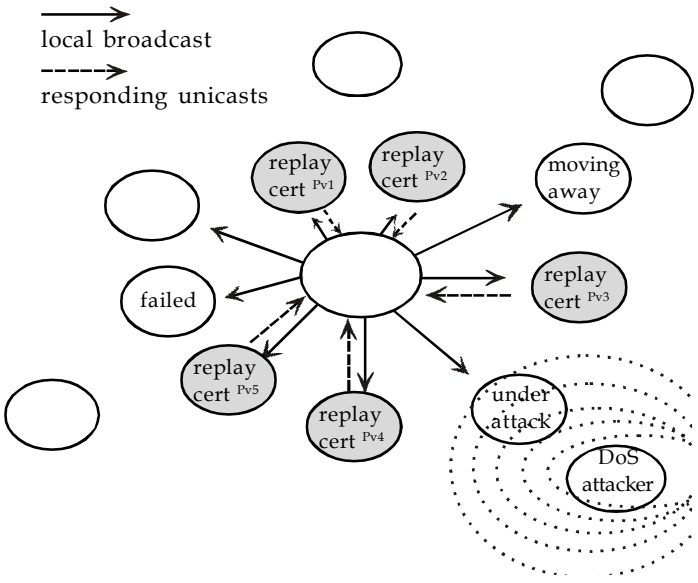

Figure 1: Dynamic Coalescing

The certificate signing key SK (in partial form) is distributed to each node of the network. A valid certificate signed by SK is obtained by combining together partial certificate shares from k (threshold) number of nodes. A node trying to establish route with some other node should have a valid certificate. Nodes without valid certificates are treated as adversaries and are precluded from using network resources. These certificates carry expiration time, after which a node has to acquire a new certificate because the old one is not valid anymore. A broken or a misbehaving node that is detected by its neighbour will not be able to get its certificate renewed, once it current certificate expires.

If the requesting node is not able to acquire the certificate shares from the threshold number of other nodes in its one-hop vicinity, it should move to a new location where it is likely to get the certificate shares. But mobility may not always be possible given the nature of the wireless ad hoc networks, that the network might be deployed in a hostile environment .

Here in these circumstances of passive and active attackers we cannot assume that we will be communicating with a trusted node every time. Hence it is very difficult to detect misbehaving nodes within the radio range, on the basis of technology available. So we use an alarm method in which when a node comes to know that an intrusion is in progress on itself, then it will issue a request for other nodes to detect if a similar nature of intrusion is taking place on them as well and also the mobile IDS agent will pass the essential information to other trusted neighbour so that the intrusion in progress cannot proceed further. Now this misbehaving node could easily deny an intrusion in itself by using mobile intrusion detection system working on itself.

CONCEPT OF TRUST

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.

DESIGN OF DISTRIBUTED TRUST MODEL

This new method of using trust as a deciding factor for design and development of secure systems provides a trust model security which can be directly applied on the distributed networks to reduce the probability of a node for being attacked or being compromised and hence improves routing.

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.

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 access control and electronic commerce. Ngai, Lyu and Chin proposed an authentication service against dishonest nodes in MANET, by applying Beth, Borcherding and Klein's trust evaluation model designed in. In Beth, Borcherding and Klein's approach, two types of trust are measured: direct trust and recommendation trust. Pirzada and McDonald 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 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.*, proposed a pair-wise trust evaluation scheme in MANETs. Jared Cordasco *et al.*, 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 and Prasant Mohapatra covered up various issues and challenges in the trust computation and propagation of trust in a hostile environment. Jin-Hee Cho, and Ananthram Swami worked on Trust-based Cognitive Networks and gave their views on Trust Management for Mobile Ad Hoc Networks.

SHARED TRUST EVALUATION MODEL

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".

Trust Quantification and 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

$$Tg = \frac{\Sigma_1^n TliW}{n} \quad \text{------ 1}$$

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

$$Tli = {}^{1/n}\left[\frac{Wi}{Wi+Ti}\right] \quad \text{------ 2}$$

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.

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

$$D = Tl - Tthreshold \quad \text{-------} \ 3$$

If D>=0, it means the computed trust value satisfies the trust requirement of the

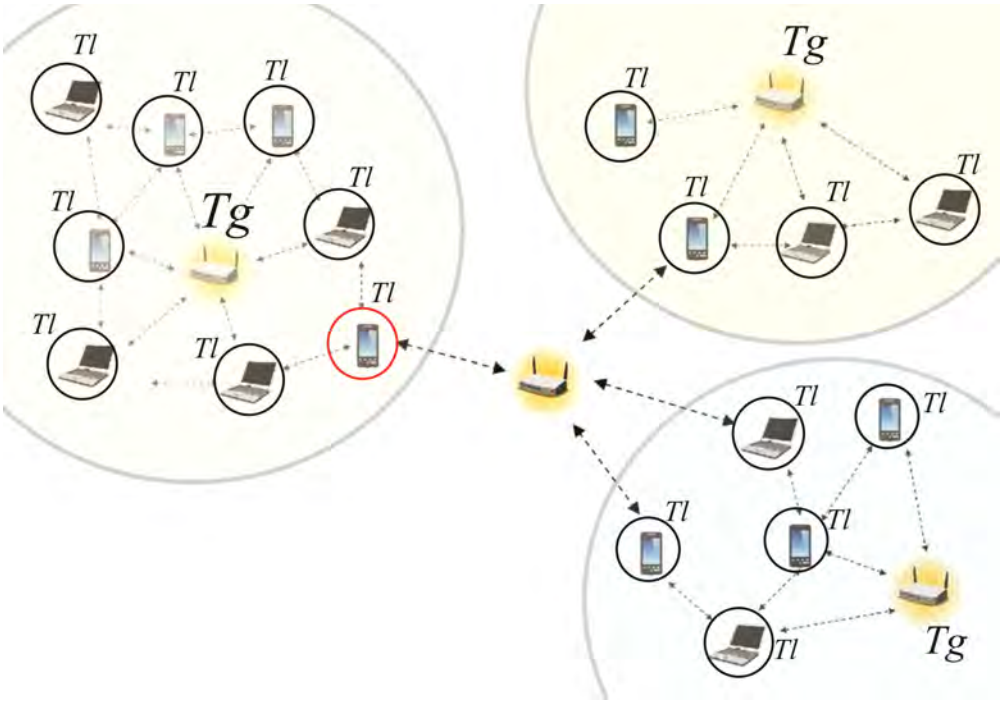

Figure 2: Distributed Trust Model

ongoing task. If D<0, it means that the trust requirement is not satisfied.

WORKING OF SHARED TRUST MODEL

Our model is an improvement of our previous work and is designed to provide flexible and effective trust evaluation for dynamic distributed 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 local security system installed at the devices, 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 certificate. To avoid such cases the decision factor uses a global dynamic threshold value to guarantee the node to stay in the communication otherwise it will be moved out of 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.

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 communication between 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 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] Perrig, R. Canetti, D. Tygar and D. Song, The TESLA Broadcast Authentication Protocol, RSA CryptoBytes, 5 (Summer), 2002.

[2] 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.

[3] 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.

[4] Grandison, T.W.A., Trust Management for Internet Applications, in Department of Computing. 2003, University of London: London, British. p. 252.

[5] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, "Self-securing ad hoc wireless networks", Seventh IEEE Symposium on Computers and Communications (ISCC_02)

[6] 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.

[7] 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.

[8] Jin-Hee Cho, Ananthram Swami, "Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks" Army Research Laboratory – Computer and Information Sciences Directorate, 14th ICCRTS, "C2 and Agility".

[9] 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.

[10] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey"

[11] 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.

[12] 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.

[13] 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.

[14] Manchala, D.W., E-commerce trust metrics and models. IEEE Internet Computing, IEEE 2000. 4(n2): p. p 36-44.

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

[16] 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.

[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] 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.

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

[20] S. Bhardwaj, S. Aggarwal and S. Goel, A Novel Technique of Securing Mobile AdhocNetworks using Shared Trust Model, International Journal of Information and Computation Technology.ISSN 0974-2239 Volume 3, Number 9 (2013), pp. 909-916

[21] Sundaram A., "An Introduction to Intrusion Detection", http://www.acm.org/crossroads/xrds2-4/intrus.html

[22] Tiranuch Anantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Wireless/ Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 – 196.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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