Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Trust Evaluation in Mobile Ad-hoc Networks

[1]Ms.D.Kalaivani and [2]Dr.V.Valli Mayil
[1]AP(SG)/MCA, Vivekanandha Institute of Information and Management Studies, Tiruchengode, India
[2]Head & Associate Professor, Dept. of Computer Science and Applications,Periyar Maniammai University, Thanjavur

Abstract: Infrastructure-less networks have become popular due to wide availability of wireless devices in everyday life. MANETs are becoming more and more common due to their ease of deployment. Mobile Ad Hoc Network is self-configuring and self-organizing wireless network of autonomous mobile devices without any central control and infrastructure. The absence of any central coordination mechanism and open nature makes the Mobile Ad Hoc Network more vulnerable to security threats. In MANET, there is a high possibility that the intermediate nodes can be malicious and they might be a threat to the security. Wormhole is the most frequently occurring attack in ad hoc networks in which one malicious node tunnels the packets from its location to other defective nodes. In this paper, we have surveyed some existing cluster-based techniques for avoidance and detection of wormhole in MANET.

Keywords: *Wormhole, Packet, Mobile Node, Malicious Node.*

I. INTRODUCTION

A mobile ad hoc network is a collection of nodes with no infrastructure while its nodes are connected through wireless links. Nodes in the network are able to discover their neighbor nodes. They communicate with each other by forwarding packets hop by hop in the network. The topology of the ad hoc network is dynamically changes as the nodes are often mobile. The success of MANET communication highly relies on the collaboration of the involved mobile nodes. Infrastructureless nature, Wireless medium and dynamic topology make MANET vulnerable to a wide range of security attacks. A major challenge in the design of the mobile ad hoc network is to protect its vulnerability from security attacks. Most of the routing protocols do not provide strong security mechanism against various attacks because of treating the nodes trustable. This lack of security provides opportunities for the attackers to conduct a wide range of attacks on the ad hoc networks. One of such security threats at network layer which degrades the performance of the network is wormhole attack. A wormhole attack is equally worse a threat for both proactive and on-demand routing protocols. In this paper, we study clustering methods of wormhole avoidance and detection in MANET.

II. WORMHOLE ATTACK

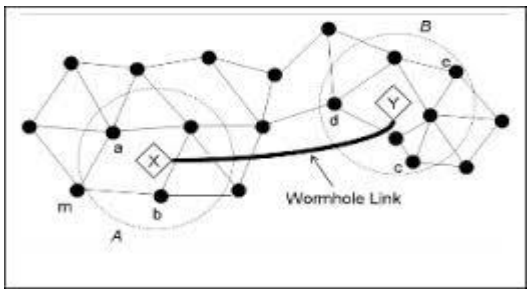

Figure 1: Wormhole Attack

A MANET is a mobile ad hoc network consists of autonomous nodes that communicate among them through wireless links in open nature. Security is a major issue for MANET due to its vulnerable characteristics. A defective node operating in the network receives packets at one location and tunnels them to another location in the network, where these packets are modified and resent into the network. The tunnel established between two attackers is referred to as a wormhole. The wormhole nodes may falsify the route by disturbing the true topology of the network and affect the throughput of the network.

III. TRUST BASED SOLUTIONS IN MANET

Many researchers have proposed the mechanisms to enhance the security, misbehavior detection as well as trust management. Trust is a value that is calculated on the basis of nodes action during communication. Various attacks like wormhole, black-hole, DOS, selfish attack have been prevented using trust based mechanisms. The nodes monitor the behavior of their neighbors while sending and receiving packets and inform the other nodes of the network about it. Each node calculates the trust value about its neighbors with the help of other nodes around them. When the trust level of a node falls below certain threshold, it is isolated from the network. The different trust models use different formula to evaluate trust value and use different ways to share trust among the nodes. The aim of a system for the node is to be able to find the safe route for sending own packets by preventing misbehaving nodes in the network. In this section, various reputation and trust-based systems for MANET are reviewed. Measuring the trust value of a node is always a challenging problem. A node's trustworthiness determines the quality of services it provides to others. There are two approaches in the quality of service.

Objective Trust

If the quality of a service can be objectively measured, then an entity's trustworthiness for that service is known as objective trust.

Subjective Trust

The subjective trust is classified into two namely direct and indirect trust relationships. Each node has a direct trust relation with the nodes located within its transmission range. The direct trust relation can be calculated through monitoring the behavior of the neighbors while finding routes. The indirect trust relation is concerned with the nodes located out of node's transmission range. One of the methods to compute the indirect trust relation is flooding the network with request messages and waiting for replies. Evaluating the trust for all the nodes needs more bandwidth, energy and delay in the route discovery process. Possible events that can be recorded in passive mode are the measure and accuracy of:

1. Frames received
2. Data packets forwarded
3. Control packets forwarded
4. Data packets received
5. Control packets received
6. Streams established
7. Data forwarded
8. Data received

Types of Trust

Functional Trust : Trusted node performs the function.
Referral Trust : Trusted node recommends another node that can perform the function.
Direct Trust : Experience of a node.
Indirect Trust : Obtained from recommendations.

Several existing secure routing in ad hoc networks are based on key management or heavy encryption techniques. These approaches for making ad hoc routing secure are more expensive and not suitable for mobile ad hoc networks because of its properties such as limited power, limited computational capabilities and limited memory for storing security information. In this section, various trust based secure ad hoc routing protocols are discussed.

TRUST AXIOMS

In this section, the meaning of trust will be explained and axioms will be presented for establishing trust relationship. The different aspects of trust are summarized as follows.

1. Trust is a relationship established between two entities for a specific action. In particular, one entity trusts the other entity to perform an action. In this work, the first entity is called the subject and the second entity is called the agent. We introduce the notation **Subject:Agent;** action to describe a trust relationship.
2. Trust can be measured by uncertainty. Here are three special cases.

A. When the subject believes that the agent will perform the action for sure, the subject fully trusts the agent and there is no uncertainty.

B. When the subject believes that the agent will not perform the action for sure, the subject fully distrusts the agent and there is no uncertainty either.

C. When the subject has no idea about the agent at all, there is the maximum amount of uncertainty and the subject has no trust in the agent. Indeed, trust is built upon how certain one is about another on whether some actions will be carried out or not. Therefore trust metrics should describe the level of uncertainty in trust relationship.

3. Trust is not necessarily symmetric. The fact that A trusts B does not necessarily means that B also trusts A, where A and B are two entities.

Trust Metrics

How to measure uncertainty in trust relationship? Information theory states that entropy is a nature measure of uncertainty. A trust metric based on entropy need to be defined, while it gives trust value 1 in the first special case, -1 in the second special case, and 0 in the third special case.

Let T {subject : agent, action} denote the trust value of the trust relationship {subject : agent, action}, and P{subject : agent, action} denote the probability that the agent will perform the action in the subject's point of view. We define the entropy-based trust value as:

$$T\{\text{subject : agent; action}\} = \begin{cases} 1 - H(p); & \text{for } 0.5 <= p <= 1; \\ H(p) - 1; & \text{for } 0 <= p <= 0.5; \end{cases}$$

where $H(p) = -p \log_2(p) - (1 - p) \log_2(1 - p)$ is the entropy function and $p = P\{\text{subject : agent, action}\}$.

This definition considers both trust and distrust. In general, trust value is positive when the agent is more likely to perform the action ($p > 0.5$), and is negative when the agent is more likely not to perform the action ($p < 0.5$). This definition also tells that trust value is not a linear function of the probability. It is also noted that (1) is a one-to-one mapping between T{subject: agent, action} and P{subject : agent, action}.

Axiom 1: Concatenation propagation of trust does not increase trust

It is well known that uncertainty does not decrease after processing. Thus, when the subject establishes a trust relationship with the agent through the recommendation from a third party, the trust value between the subject and the agent should not be more than the trust value between the subject and the recommender as well as the trust value between the recommender and the agent. The method for calculating trust via concatenation is referred to as entropy-based trust models.

Axiom 2: Multipath propagation of trust does not reduce trust

If the subject obtains an extra recommendation, which agrees with the subject's current opinion, the subject will be more certain about the agent, or at least maintain the same level of certainty. Thus, if the subject receives the same recommendations for the agent from multiple sources, the trust value should be no less than that in the case where the subject receives less number of recommendations.

Axiom 3: Trust based on multiple recommendations from a single source should not be higher than that from independent sources

When the trust relationship is established jointly through concatenation and multipath trust propagation, it is possible to have multiple recommendations from a single source, as shown in Figure 2 (a). Since the recommendations from a single source are highly correlated, the trust built upon those correlated recommendations should not be higher than the trust built upon recommendations from independent sources.

Entropy-based Trust Model

In this model, the trust propagations are calculated directly from trust values. For concatenation trust propagation, node B observes the behavior of node C and makes recommendation to node A as T_{BC} = {B : C; action}. Node A trusts node B with T{A : B; making recommendation} = R_{AB}.

Probability-based Model

In the second model, concatenation and multipath trust propagation is calculated using the probability values of the trust relationship. The probability values can be easily transferred back to trust values. For the concatenation trust propagation, let $_{pAB}$ denote P{A : B; make recommendation}, $_{pBC}$ denote P{B: C; action} and $_{pABC}$ denote P{A : C; action}. We also define $_{p'B}$ as the probability that B will make correct recommendations, $_{p'C|B=1}$ as the probability that C will perform the action if B makes correct recommendation.

IV. DESIGNING BEST MODEL FOR MANET

- The trust model should be infrastructure-less. Because the network routing infrastructure is formed in an ad-hoc fashion, the trust management cannot depend on, e.g., a trusted third party (TTP) such as public key infrastructure (PKI) and certification authorities (CA) or registration authorities (RA) with elevated privileges etc.
- The trust model should be anonymous because of the anonymity of mobile nodes in MANETs.
- The trust model should be robust to all kinds of attacks and to the presence of malicious nodes.
- Computation, storage, and complexity overheads of the trust model should be minimal.
- The trust model should be self-organized. MANETs are characterized to have dynamic, random, rapidly changing and multi-hop topologies composed of relatively.

CONCLUSION

Trust based solutions can protect the mobile ad hoc networks against wormhole problem and thus increase its performance. Here, we have analyzed some trust evaluation models to provide better solutions for mobile ad hoc networks.

References

[1] D. B. Johnson and D. A. Maltz, "Dynamic source routing protocol in ad hoc wireless networks," in Mobile Computing, T. Imielinski and H. Korth, Eds. Boston, USA: Kluwer Academic Publishers, 1996, ch. 5, pp. 153–181.

[2] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2):618–644, 2007.

[3] A. A. Pirzada, McDonald C., and A. Datta. Performance comparison of trust-based reac- tive routing protocols. IEEE Trans. on Mobile Computing, 5(6):695–710, 2006.

[4] G. Theodorakopouls and J.S Baras, ―Trust Evaluation in ad-hoc networks, in ACM Workshop Wireless security, Oct. 2004.

[5] Z. Yan, P. Zhang and T. Virtanen, ―Trust Evaluation Based Security Solution in Ad Hoc Networks‖, 3rd International Semantic Web Conference, 2004.

[6] Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs" IEEE 978-1-61284-307-0/11/2011.

[7] Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia, Wormhole Attack Detection in Mobile Ad Hoc Networks, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[8] D. E. Denning, "A new paradigm for trusted systems," Proceedings on the 1992-1993 workshop on New security, 1993.

[9] A. A. Pirzada and C. McDonald, "Dependable dynamic source Routing without a trusted third party," Journal of Research and Practice in Information Technology, vol. 39, issue 1, February 2007.