Trust Model in MANET : An Overview

Nimitr Suanmali
Suan Dusit Rajabhat University
295 Rajasima rd. Dusit Bangkok
nimitrs@hotmail.com

Kamalrulnizam Abu Bakar
Department of Computer System and Communication
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia
kamarul@fsksm.utm.my

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a temporarily formed network, created, operated and managed by the nodes themselves. It is also often termed an infrastructure-less, self-organized, or spontaneous network. The applications of MANET are widely use in an industrial, commercial, or military because it provided much more flexible and inexpensive network. As each node in the network forward data and control packets from one node to another in the range of wireless signal make MANET easy to eavesdropping. The existence of a network is solely depended upon the cooperative and trustworthy of nodes in the network. Similarly, the security of nodes in MANET depended on the participation and trustworthiness of neighbor nodes in the network. A MANET is vulnerable to many sources of attacks by adversary nodes, internal and external source. Many trust mechanisms have been develop to overcome these attacks but depend on a central trust authority that impractical requirement for MANET. This paper presented several trust models in MANET environment based on trustworthiness of peer nodes. It concentrated on providing a brief overview of trust model and identifying type of attacks related to trustworthiness of node in MANET.

Categories and Subject Descriptors

A.1[General Literature]: Introductory And Survey

General Terms

Security

Keywords

Trust Management, Security, MANET

1. INTRODUCTION

The growth of wireless computer networks plays increasingly vital roles in modern society. Self organization, lacks of infrastructure, and dynamic change of nodes are the main characteristic of Mobile Ad Hoc Network (MANET). A MANET is a collection of wireless mobile nodes performing a temporary network without any established infrastructure or centralized authority[1]. Such network does not rely on fixed architecture and pre-determined connectivity. Nodes transmit information directly to another in range of their wireless signal. The transmission range depends not only on the power level used for the transmission, but also on the terrain, obstacles and the specific scheme used for transmitting the information[2]. The intermediate nodes will be used to forward packets from source node to destination node. Nodes in MANET are dynamically change which means that the topology of such networks may change rapidly and unpredictably over time. A MANET consist of devices that are autonomously self-organized into networks. With a self-organizing capability, which makes MANET completely different from any other network. MANET is one of the most innovative and challenging areas of wireless networks. It is a key step in the evolution of wireless networks. MANET is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. The network is a self-organization which means that all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The main challenge of MANET is the vulnerability to security attacks. The security challenge has become a primary concern to provide secure communication.

The remaining of this paper is organized as follow. In section 2, described about trust and security issues. In section 3, gives the information of some attacking on MANET. In section 4, provide a brief overview of related work on trust model. In section 5, gives a discussion of trust model. At last, we conclude and point out the future work.

2. Trust and Security Issues

Trust and security play a key role in building the information security. For nodes participated in MANET, they must have confidence that their neighbor nodes are trustworthy and secure. Trust often refers to mechanisms to verify that the source of information is really who the source claims to be. Signatures and encryption mechanisms should allow any nodes to check the sources of that information. Trust and security are tightly interdependent entity that cannot be separated. For example, cryptography is depend on trusted key exchange. Likewise, trusted key exchange cannot perform without security service. This relation always used when establish a secure system.

Trust in wired networks is usually accomplished by indirect trust mechanisms with trusted certification agencies and authentication

Conference'04, Month 1–2, 2004, City, State, Country.

servers. Nevertheless, to establishing the indirect trust mechanism requires some mechanism for initial authentication and is normally behave with physical or location-based authentication schemes. Trust establishment in MANET is still an uncover and challenging field. The behavior of MANET is based on trust your neighbor relationships. These relationships initiate, develop and terminate dynamically and have usually short life spans. The trust relationships are extremely sensitive to attacks in such networks. There are many of reasons that some nodes in such network can easily mould these relationships to grab required information. For a number of reasons, including better service, selfishness, monetary benefits or malicious intent, some nodes can easily mould these relationships to extract desired goals. Moreover, the absence of fixed trust infrastructure, limited resources, ephemeral connectivity and availability, shared wireless medium and physical vulnerability, make trust establishment virtually impossible. To overcome these problems, trust has been established in MANET using a number of assumptions including pre-configuration of nodes with secret keys, or presence of an omnipresent central trust authority. In our opinion, these assumptions are against the very nature of MANET, which are supposed to be improvised and spontaneous.

According to [3] trust is defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the party”. Author in [4] defines trust in a passionate entity (human) as the belief that it will behave without malicious intent and trust in a rational entity (system) as the belief that it will resist malicious manipulation. Trust in entities is based on the fact that the trusted entity will not act maliciously in a particular situation. As no one can ever be absolutely sure of this fact, trust is solely dependent on the belief of the trustor. The derivation of trust may be due to direct trust based on previous similar experiences with the same party, or indirect trust based on recommendations from other trusted parties. Trust is also time dependent, it grows and decays over a period of time. A pure ad-hoc network closely resembles this human behaviour model, where a number of people/nodes that have never met each other, are able to communicate with each other based on mutual trust levels developed over a period of time. Trust cannot be treated as a property of trusted systems but rather it is an assessment based on experience that is shared through networks of people [5]. As in real life, trust levels are determined by the particular actions that the trusted party can perform for the trustee. Similarly trust levels can be computed based on the effort that one node is willing to expend for another node. This effort can be in terms of battery consumption, packets forwarded or dropped or any other such parameter that helps to establish a mutual trust level. A trust model that is based on experience alone may not be secluded from attacks in an ad-hoc network but it can identify routes with a certain measure of confidence.

3. Type of Attacks on Trust in MANET

Attacks on network come in many varieties and they can be grouped based on different characteristics. Many researcher used different aspect to classified the attacks on MANET, the researcher in[6] classified the attack based on the trustworthiness of communication partner in the network. They divided the attacks on MANET into two main catagories by their sources, external attacks and internal attacks.

- In external attacks, the attacks are committed by the nodes that are not legally part of the network. The attackers are necessary to compromise one node in the target network. The target nodes might be a self-sufficient node that link to entire network using the same infrastructure or communication link. The compromised node would be use to initiate attack in the target network without even being authenticated. All network communication in the target network will be possible to break down by the attacker from outside through the compromised node. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on.

- Internal attacks are typically more severe attacks, the source of attacks are come from inside a particular network. A malicious inside node already belong to the network as an authorized party. A malicious node with access to all nodes in its range might pose a crucial threat to the capability of the whole network. Since the internal attacks are not easy to prevent, the attacks can be performed more efficiently. Moreover, the malicious nodes that is part of the network which assumed to be trusted by entire nodes might be use the standard security means to actually protect their attacks.

3.1 Impersonation Attacks

Impersonation attacks[6] are also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can easily join or he could remove security measures to allow subsequent attempts of invasion. A compromised node may also have access to encryption keys and authentication information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information. Attackers might see an advantage in selectively forwarding packets that pass them. An intruder will most likely try to impersonate a node within the path of the data flow of interest. It could achieve this by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel. Depending on the layer where the identity faking takes place, it can be difficult to prevent it. Exploiting MAC layer protocol weaknesses, attackers could place their node between two other nodes communicating with each other (man-in-the-middle attack). Since MAC addresses can be faked with little effort, detecting an illegitimate intruder might not be possible in this layer. However, by using good authentication algorithms, strong data encryption and secure routing protocols, the effects of impersonation can be reduced significantly.

3.2 Sybil Attacks

Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes, by doing so undermining the redundancy of many routing protocols. This attack called sybil attack[6]. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have a harder time to destroy the integrity of information. If the same packet is sent over several distinct paths, a change in the packets incoming from one of these paths can be detected easily, thus isolating a possible intruder in the network becomes possible. Also, if not the same packet but pieces of related information are sent on distinct routes, an eavesdropper might have difficulties putting together the pieces of the information puzzle. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded. The attacker may get access to all pieces of the fragmented information or may alter all packets in the same transmission so that the destination nodes cannot detect tampering anymore. In trust-based routing environments, representing multiple identitities can be abused to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it to starting point for further attacks. By using unique symmetric keys, each node can verify its neighbors identity, and limiting the number of neighbors a node can have results in the partial isolation of compromised nodes, since they can only communicate with their verified neighbors.

4. Existing Type of Trust Models

In this section, we describe the trust models that suitable for application to MANET based on the concept of trustworthiness of peer nodes.

4.1 Distributed Public-Key Model

The Distributed Public-Key Model[7] makes use of threshold cryptography to distribute the private key of the Certification Authority over a number of servers. An (n, t+1) scheme allows any t+1 servers out of total of n servers to combine their partial keys to create the complete secret key. Similarly, it requires that at least t+1 servers must be compromised to acquire the secret key. The scheme is quite robust but has a number of factors that limit its application to pure ad-hoc networks. Primarily it requires an extensive pre-configuration of servers and a distributed central authority, secondly the t+1 servers may not be accessible to any node desiring authentication and lastly asymmetric cryptographic operations are known to drain precious node batteries.

4.2 Resurrecting Duckling Model

The Resurrecting Duckling Model[8] is based upon a hierarchical graph of master-slave relationships. The slave (duckling) considers the first node that sends it a secret key through a secure channel as its master (mother duck). The slave always obeys the master and gets all instructions and access control lists from its master. The slave further becomes a master to other devices with whom it can share a secret key through secure means. This master-slave bond can only be broken either by a master, a timeout or an event, after which the slave is no longer bonded and looks for another master. This model is most suitable for security in large-scale dumb sensor nodes where pre-configuration has to be avoided. As this model uses a hierarchical security chain it is not appropriate for application to ad-hoc networks.

4.3 Friend Recommendation Model

The Friend Recommendation Model[9] is based on a trust chain between nodes in network to create trusted community. A pair of friend nodes, which assumed to have a mutual trust between them before joining the network, are capable of creating a security association between them to participate in MANET operations. The friendship mechanism is able to speed up the creation process of a trusted community in the network. Each node needs to meet and establish mutual trust with other nodes, which requires a lot of time and effort. In friend recommendation if node A wishes to have a trust relation with node B, node A needs to have at least one node in node B's friend list, node C, to authenticate its identity. If there is no node in B's friend list that has physically met node A before, the recommendation request will then be forwarded to the next hop in the same manner. When a node that knows the identity of node A is found, the information is sent back to node B to complete the authentication process. However, if no one in the chain knows about node A's identity, node A then must name at least one node, node D, that it has met before to act as a reference node. Node B then will do the same process to authenticate node D's identity. If the identity of node D is known by any node B's friends in the chain list, the identity of node A then is considered authenticated.

4.4 Localized Trust Model

The localized trust model[10] is based on trustworthiness of node by their own local community. In localized trust model, an entity is trusted if any k trusted entities claim so within a certain time period T_{cert}. These k entities are typically among the entity's one-hop neighbors. Once a node is trusted by its local community, it is globally accepted as a trusted node. Otherwise, a locally distrusted entity is regarded as untrustworthy in the entire network. K and T_{cert} are two important parameters with T_{cert} characterizing the time-varying feature of a trust relationship. The options for setting k is to set k as a globally fixed parameter that is honored by each entity in the system. In this case, k acts as a system-wide trust threshold. The k parameter is tuned according to the network density and system robustness requirements. If a node could not find k neighbors in certain location, it may roam to meet more nodes or wait for new nodes to move in. They developed a scalable share update scheme , optimization techniques that greatly enhance the efficiency and robustness of their algorithms and protocols . As this model has scalability feature architecture to facilitate practical deployment in a potentially largescale network with dynamic node membership it is suitable for application to ad hoc networks.

4.5 Bayesian Network-Based Model

The Bayesian Network-Based Model[11] is focused on trust and reputation of node in the network based on a Bayesian Network Model. A trust value of a one node is more valuable to other nodes. A node build two kinds of trust in another node, trust in competence in providing service and trust in reliability in providing recommendation about others node. Since nodes are heterogeneous, they judge other's node behavior by different criteria. One node can trust another node if their criteria are similar. Even though both node tell the truth, they can not trust each other if their criteria are different. A Bayesian network is a relationship network that uses statistic methods to represent probability relationships between different elements. Each Bayesian network has a root node T, which has two values, "satisfying" and "unsatisfying", denoted by 1 and 0, respectively. Each node called leaf node is associated with a conditional probability table (CPT). Once getting nodes' CPTs in a Bayesian network, a node can compute the probabilities that the corresponding root node is trustworthy in different aspects by using Bayes rules. Nodes can set various conditions according to their needs. With the Bayesian networks, nodes can infer trust in the various aspects that they need from the corresponding probabilities. That will save nodes much effort in building each trust separately, or developing new trust when conditions change. After each interaction, nodes update their corresponding Bayesian networks. As this model provided an easy way to present a complex and correlative relationship of nodes, this model is suitable in both small and large size MANET.

5. Discussion

In this section we give a discussion of trust model on some key feature that could be provide more reliable of trust relationship in MANET. As show in table 1, we selected 3 main key features to give a discussion with trust model. These features are the main concerns of resource constraint in MANET environment. Since, the lightweight feature is the main concern in limited resources of node. The need of complex computational mechanism should be eliminate. A MANET operates in the self-organization manner, the use of fixed infrastructure must be avoid. In addition, the use of certificate authority is not useful in MANET environment. Also, the scalable feature provided a flexible trust mechanism to secure nodes in both small and large scale MANET. We will give a brief discussion on each trust model respectively.

Table 1 Key feature of trust model

Model	Self Organize	Light Weight	Scalable
Distributed Public Key	no	no	yes
Resurrecting Duckling	yes	yes	yes
Friend Recommendation	yes	yes	no
Localized Trust Model	yes	no	yes
Bayesian Network-Based	yes	yes	yes

Distributed Public Key Model : this model does not support the self-organization feature because it used threshold cryptography that rely on a certification authority (CA). This scheme is quite robust but has many factors that limit its application to MANET. Similarly, with the use of threshold cryptography, this model does not support the light weight too. For the scalable feature, this model can be apply in both small and large size network. The advantage of this model is the used of threshold cryptography that make this trust model is robust and the key of the service is confidential. Even though this model provided robust mechanism and confidential key, this trust model is not suitable to apply to MANET.

Resurrecting Duckling Model : this model is based on a master-slave relationships that supported the self-organization feature because the mechanism to building relationships between master and slave can be established by themselves through a secure channel without any central infrastructure. The relationship between master and slave initiated with share secret key mechanism that operated through secure channel without the need of complex computational mechanism. Also, with the scalable feature, the relationship between master and slave can be delegate to other device in a large scale network. Although, this model is most suitable for a large-scale sensor network, it is not suitable for MANET network.

Friend Recommendation Model : this model is based on a trust chain between nodes in a network. The trust chain mechanism of this model operates by the node themselves without any central authority that supported the self organization feature. This model provided the lightweight feature by using a simple mechanism to make a trust chain of each node. Each pair of friend nodes need to meet together and assumed to have a mutual trust before joining a network. This model overcome the sybil attacks, the identity theft attack, by a physical meeting of two nodes before they established trust relationships. Even though this trust model can be apply to a large scale network, the computation of trust chain mechanism will take a long time.

Localized Trust Model : this model is based on concept of localize certification service that operates in every node. This service supported the self organization feature. Although, the certification service can be perform in every node to authenticate users that roaming from another network. The result of evaluation show that computation power is a critical factor of the performance when process with the low-end processor device. The underlying cryptographic primitives make this model can be handle the impersonation attacks from adversaries. Even though, this model can be apply to a large scale MANET network, nodes in network should be a high performance devices.

Bayesian Network-Based Model : this model based on Bayesian network that provide a flexible method to present distinct trust with different aspects of node. The trust mechanism of node developed by a naïve Bayesian network that operates in self organization manner. Likewise, the trustworthiness of neighbor node can be compute by using Bayes rules. Moreover, with lightweight feature, each node can infer trust from the corresponding probability table that will save nodes much effort in building or developing new trust when conditions change. This trust model can be scalable to apply to both small and large network under the condition that the small-world phenomenon[12] happens.

6. Conclusions

Trust model was introduced for many years, but its development is not over yet. Several trust models have been invented to prevent attacks from untrust party but they required massive computation from MANET device that has many physical constrains, battery, memory, cpu and so on. The attributes of MANET make conventional trust model even more difficult to apply to them. In this paper, We have identified some attacks related to trustworthiness of peer and given a brief overview of existed trust model in MANET. We have discussed the relevance of each of these area to important aspects of ongoing and future research of trust model.

7. REFERENCES

[1] S. Alampalayam, A. Kumar, and S. Srinivasan, "Mobile ad hoc network security-a taxonomy," Advanced Communication Technology, 2005, ICACT 2005., 2005.

[2] F. Anjum and P. Mouchtaris, Security for Wireless Ad--hoc Networks: John Wiley & Sons, 2006.

[3] R. Mayer, J. Davis, and D. Schoorman, "An Integrative Model of Organizational Trust," The Academy of Management Review, vol. 20, pp. 709-734, 1995.

[4] A. Jøsang, "The right type of trust for distributed systems," Proceedings of the 1996 workshop on New security paradigms, 1996.

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

[6] A. Burg, "Ad hoc network specific attacks," Seminar Ad hoc networking, Technische Universitaet Muenchen, 2003.

[7] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, 1999.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," Security Protocols: 7th International Workshop, Cambridge, 2000.

[9] S. A. Razak, S. Furnell, N. Clarke, and P. Brooke, "Building a Trusted Community for Mobile Ad Hoc Networks Using Friend Recommendation," Springer, 2007.

[10] J. Zhung, H. Luo, and P. Zerfos, Selfsecuring ad hoc wireless networks: ISCC, 2002.

[11] Y. Wang and J. Vassileva, "Bayesian network-based trust model," Proceedings of the IEEE/WIC International Conference on Web Intelligence (WI'03), 2003.

[12] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proceedings of the 32nd ACM Symposium on Theory of Computing, 2000.