A CONFIDENCE MODEL BASED ROUTING PRACTICE FOR SECURE ADHOC NETWORKS

Ramya. S[1] and Prof. B. Sakthivel[2]

ramyasiva.jothi@gmail.com and everrock17@gmail.com
[1]PG Student and [2]Professor & Head, Department of Computer Science and Engineering
P.S.V. College of Engineering & Technology, Krishnagiri.

---***---

Abstract - Security issues have been stressed when versatile specially appointed systems (MANETs) are utilized into militaryand aviation fields. In this paper, we plan a novel secure steering convention for MANETs. This convention TAODV(Trusted AODV) broadens the generally utilized AODV (Ad hoc On demand Distance Vector) steering convention and utilizes theidea of a trust model to secure directing practices in the system layer of MANETs. In the TAODV, trust among hubs is represented by supposition, which is a thing gotten from abstract rationale. The sentiments are dynamic and refreshed frequently as our convention particular: If one hub performs normal communications, its assessment from other hubs' purposes of view can be expanded; something else, on the off chance that one hub plays out some pernicious practices, it will be at last denied by the entire system. A trust proposal instrument is likewise designed to trade trust data among hubs.

Key Words: *AODV, MANET's, TAODV*

1. INTRODUCTION

A mobile ad hoc network (MANET) is a kind of wireless network without centralized administration or fixed network infrastructure, in which nodes perform routing discovery and routing maintenance in a self-organized way. Nowadays MANET enables many promising applications areas of aerospace and military. Due to some of its characteristics such as openness, mobility, dynamic topology and protocol weaknesses, MANETs are prone to be unstable and vulnerable. Consequently, their security issues become more urgent requirements and it is more difficult to design and implement security solutions for MANETs than for wired networks. Many security schemes from different aspects of MANETs have been proposed, such as secure routing protocols and secure key management solutions. However, most of them assume centralized units or trusted third-parties to issue digital certificates, which actually destroy the self-organization nature of MANETs. And by requiring nodes to request and verify digital signatures all the time, these solutions often bring huge computation overheads. Our solution is, on the other hand, a secure routing protocol which employs the idea of a trust model so that it can avoid introducing large overheads and influencing the self-organization nature of MANETs. In this paper, we apply the trust model into the security solutions of MANETs. Our trust model is derived and modified from subjective logic, which qualitatively defines the representation, calculation, and combination of trust. Trust models have found security applications in e-commerce, peer-to-peer networks, and some other distributed systems. In recent years, some research work is conducted to apply trust models into the security solutions of MANETs. However, there are no concrete and applicable designs proposed for the security of routing protocols in MANETs, to the best of our knowledge.

2. BACKGROUND

Subjective logic is a kind of trust model which was proposed by A. Josang. It is "a logic which operates on subjective beliefs about the world, and uses the term opinion to denote the representation of a subjective belief". The trust between two entities is then represented by opinion. An opinion can be interpreted as a probability measure containing secondary uncertainty. In MANET, nodes move with high mobility and may experience long distance in space among each other. A node may be uncertain about another node's trustworthiness because it does not collect enough evidence. This uncertainty is a common phenomenon, therefore we need a model to represent such uncertainty accordingly. Traditional probability model, which is also used in some trust models, cannot express uncertainty. While in subjective logic, an opinion consists of belief, disbelief and also uncertainty, which gracefully meets our demands. Subjective logic also provides a mapping method to transform trust representation between the evidence space and the opinion space. Our trust model used in TAODV is then derived and modified from the subjective logic and is more applicable for the instance of MANET. In the subjective logic, an opinion includes four elements. The fourth one is relative atomicity. Ad hoc On-demand Distance Vector Routing Protocol Ad hoc On-demand Distance Vector (AODV) routing protocol is one of the most popular routing protocols for MANETs. On demand is a major characteristic of AODV, which means that a node only performs routing behaviours when it wants to discover or check route paths towards other nodes. This will greatly increase the efficiency of routing processes. Routing discovery and routing maintenance are two basic operations in AODV protocol. Routing discovery happens when a node wants to communions. These mechanisms have been proposed in some previous work, such as intrusion detection system in and watchdog technique in. Another kind of secure routing protocol which uses cryptography technologies is recommended to take effect before nodes in the TAODV establish trust relationships among one another and are the latest security schemes for securing MANET, which employ cryptography technologies. We assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures.

3. OVERVIEW OF THE TRUSTED AODV (TAODV)

Network Model and Assumptions In this work, we make some assumptions and establish the network model of TAODV. We also argue why we focus our security solution on routing protocol in the network layer. Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. We do not concern the security problem introduced by the instability of physical layer or link layer. We only assume that: (1) Each node in the network has the ability to recover all of its neighbors; (2) Each node in the network can broadcast some essential messages to its neighbors with high reliability; (3) Each node in the network possesses a unique ID, the physical network interface address for example that can be distinguished from others. In the TAODV, we also assume that the system is equipped with some monitor mechanisms or intrusion detection units either in the network layer or the application layer so that one node can observe the behaviors.

Framework of the Trusted AODV

There are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on our trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating. The structure and relationship among these components are shown in Figure1. The general procedure for establishing trust relationships among nodes and for performing routing discovery is described as follows. Let us first imagine the beginning of an ad hoc network which contains a few nodes. Each node's opinion towards one another initially is (0,0,1), which means that the node does not trust or distrust another node but it is only uncertain about another node's trustworthiness.

4. TRUST MODEL FOR TAODV

Trust Representation Our trust model is an extension of the original trust model in subjective logic which is introduced in Section 2. In our trust model, opinion is a 3-dimensional metric and is defined as follows:

Definition 1(Opinion). Let denote any node's opinion about any node 's trustworthiness in a MANET, where the first, second and third component correspond to belief, disbelief and uncertainty, respectively. These three elements satisfy:

In this definition, belief means the probability of a node can be trusted by a node, and disbelief means the probability of cannot be trusted by. Then uncertainty fills the void in the absence of both belief and disbelief, and sum of these three elements.

Mapping between the Evidence and Opinion Spaces A node in MANET will collect and record all the positive and negative evidences about other nodes' trustworthiness, which will be explained in detail in Section 5. With these evidences we can obtain the opinion value by applying the following mapping equation which is derived from.

Definition 2 (Mapping). Let be node A's opinion about node B's trustworthiness in a MANET, and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness, then can be expressed as a function of p and n according to:

Trust Combination In our trust model, a node will collect all its neighbors opinions about another node and combine them together using combination operations. In this way, the node can make a relatively objective judgment about another node's trustworthiness even in case several nodes are lying. The followings are two combination operations nodes may adopt: Discounting Combination and Consensus Combination.

5. ROUTING OPERATIONS IN TAODV

Node Model We add three new fields into each node's original routing table: positive events, negative events and opinion. Positive events are the successful communication times between two nodes. Similarly negative events are the failed communication ones. Opinion means this node's belief towards another node's trustworthiness as defined before. The value of opinion can be calculated according to Formula 2. These three fields are the main factors when performing trusted routing. One node's routing table can be illustrated by Figure 2, where some fields are omitted for highlighting the main parts.

Trust Judging Rules

Before describing the process of trusted routing discovery and maintenance in detail, we predefine some trust judging rules here and in Table 1.(1) In node's opinion towards node 's trustworthiness, if the first component belief of opinion is larger than 0.5,will trust and continue to perform routing related to.(2) In node's opinion towards node 's trustworthiness, if the second component disbelief of opinion is larger than0.5,will not trust and will refuse to performing routing related to. Accordingly the route entry for in routing table will be disabled and deleted after an expire time.(3) In node's opinion towards node 's trust worthiness, if the third component uncertainty of opinion is larger than 0.5,will request 's digital signature when ever has interaction (or relationship) with .(4) In node's opinion towards node 's trustworthiness, if the three components of opinion are all smaller than or equal to 0.5,will request 's digital signature whenever has interaction (or relationship) with. (5) If node has no route entry in node's routing table's opinion about is initialized as (0,0,1).

Trust Updating Policies

Opinions among nodes change dynamically with the increase of successful or failed communication times. When and how to update trust opinions among nodes will follow some policies. We derive as follows:

(1) Each time a node has performed a successful communication with another node , including forwarding route requests or replies normally, generating route requests or route replies normally, etc., 's successful events in's routing table will be increased by .

(2) Each time a node has performed a failed communication with another node including forwarding route requests or replies abnormally, generating route requests or route replies abnormally, authenticating itself incorrectly, and so on, 's failed events in's routing table will be increased by .

(3) Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using Equation 2 from the evidence space to the opinion space.

(4) If node's route entry has been deleted from node's route table because of expiry, or there is no 's route entry from the beginning, the opinion will be set to (0,0,1).

Trust Recommendation

Existing trust models seldom concern the exchange of trust information. However, it is necessary to design an information exchange mechanism when applying the trust models into network applications. In our trust recommendation protocol, there are three types of messages: Trust RequestMessage (TREQ), Trust Reply Message (TREP), and TrustWarning Message (TWARN). Nodes who issue TREQ messages are called Requestor. Those who reply TREP messages are called Recommender.

When a node wants to know another node's new trustworthiness, it will issue an TREQ message to its neighbors. TREQmessage uses the above structure and leaves the fields of Recommender, Opinion and Expiry empty. The Type field is set to 0. Nodes which receive the TREQ message will reply with an TREP message with the Type field set to 1. When a node believes that another node has become malicious or unreliable, it will broadcast a TWARN message with the Type set to 2 to its neighbors.

Trusted Routing Discovery

We take AODV for example to illustrate how to perform trusted routing discovery using the idea of our trust model.

Scenario I: Beginning of A TAODV MANET—Let us consider a simple MANET which only contains 3 nodes:

Now suppose node wants to discover a route path to node. The processes of node, , and are listed below.

1. Broadcasts an RREQ requesting route path to , then begins waiting for an RREP from its neighbor .

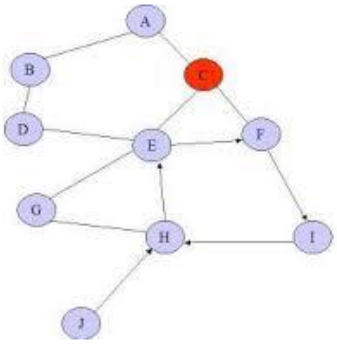

Fig. 5.1 Broadcast Nodes

6. ANALYSIS

By introducing the idea of the trust model into our design, we are able to establish a more flexible and less overhead secure routing protocol for MANETs. From performance point of view, our trusted routing protocol introduces less computation overheads than other security solutions n for MANETs. This design does not need to perform cryptographic computations in every packet, which will cause huge time and performance consumption. After the trust relationship is established, the subsequent routing operations can be performed securely according to trust information instead of certificates all the time. Therefore, the TAODV routing protocol improves the performance of security solutions. Unlike some previous security schemes [3] [4], whose basis of routing operations is "blind un-trust", TAODV do not decrease the efficiency of routing discovery and maintenance. From security point of view, our design will detect nodes' misbehavior finally and reduce the harms to the minimum extent. When a good node is compromised and becomes a bad one, its misbehavior will be detected by its neighbors. Then with the help of trust update algorithm, the opinions from the other nodes to this node will be updated shortly. Thus this node will be denied access to the network.

7. CONCLUSION AND FUTURE WORK

This paper is the first to apply the idea of a trust model in subjective logic into the security solutions of MANETs. The trust and trust relationship among nodes can be represented, calculated and combined using an item opinion. In our TAODV routing protocol, nodes can cooperate together to obtain an objective opinion about another node's trustworthiness. They can also perform trusted routing behaviors according to the trust relationship among them. With an opinion threshold, nodes can flexibly choose whether and how to perform cryptographic operations. Therefore, the computational overheads are reduced without the need of requesting and verifying certificates at every routing operation. In summary, our trusted AODV routing protocol is a more light-weighted but more flexible security solution than other cryptography and authentication designs.

REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations (rfc2501)," January 1999, http://www.ietf.org/rfc/rfc2501.txt.

[2] C. E. Perkins, Ed., Ad Hoc Networking. Boston: Addison-Wesley, 2001.

[3] Y. Teng, V. V. Phoha, and B. Choi, "Design of trust metrics based on dempster-shafer theory," http://citeseer.nj.nec.com/461538.html.

[4] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen, "Trust propagation in small worlds," in Proceedings of the 1st International Conference on Trust Management, 2002, http://citeseer.nj.nec.com/575876.html.

[5] A. Abdul-Rahman and S. Halles, "A distributed trust model," in Proceedings of New Security Paradigms Workshop '97, 1997, pp. 48–60.