Building Trust Territory In Ad Hoc Networks

Yuan Bai
Liaoning University of Technology
Jinzhou, Liaoning, China
Beijing University of Posts and Telecommunications
Beijing, China
snowbaiyuan@163.com

Xing Zhang
College of Computer Science and Technology
Beijing University of Technology, BJUT
Beijing, China
zhang_xing@emails.bjut.edu.cn

SUN Bin
Beijing University of Posts and Telecommunications
Beijing, China
sunbin@bupt.edu.cn

Abstract—Building trust has been recognized as a new security approach for wireless distributed networks. In the paper, we try to provide a completely new view by building trust territory in ad hoc networks. The concept of trust territory is addressed and the approach to build trust territory is also discussed. A trust territory contains all nodes trusted by the node. It is considered secure to communicate with nodes in the trust territories. Trusty theorie, which may not be novel the ideality. The paper extends the trust area and gives trust relationships. Trust territory could work in all layers of networks, so its potential for future applications is very promising.

Keywords-Trust; Ad Hoc Networks; trust territory; sets; relations; graphs

I. INTRODUCTION

Security is always a challenge for wireless distributed networks. With transmitting data in the air, radio waves can be easily intercepted by any attacker, which is the most significant source of risks in ad hoc networks.

Another challenge comes from the distributed nature of these networks. The lack of the center control makes distributed networks vulnerable to be attacked.

Due to these new challenges, many security solutions that are effective in a wired network become inapplicable in ad hoc networks. Building trust relationships is considered as a way to solve secure problem for distributed networks and has attracted more and more attention. [2]

Trust is a subjective expectation that an entity has about another’s future behavior based on the history of their encounters [1]. The research on trust evaluation has been extensively performed for a wide range of applications, including public key authentication, e-commerce, peer-to-peer networks, and ad hoc and sensor networks [4]. However, all studies about trust are based on certain layer and certain application. No one is thinking in whole networks society. Building a trust networks society, especially in ad hoc networks, is kind of ideality for scholars and common users. Discusses about trust territory in the paper make us closer to the ideality. The paper extends the trust area and gives trust theory, which may not be novel, a completely new view.

The paper addressed a concept of trust territory and discussed the approach to build trust territory in networks society. A certain node’s trust territory is a set containing all trusted nodes. Depending on specific application scenarios the node could be web server, router, users etc.

The idea of trust territory is from the experiences in social society. In our social society, each person has his own trust territory although we seldom use the term of “trust territory”. The relatives and friends compose our trust territory. We ask for help from people in our trust territory when we are in trouble. The recommendation from trust territory is tending to be acceptable. The same thing also happens in networks society. If a node in networks built a trust territory, it can select the nodes in its trust territory to do some specific actions, such as changing data, do business or routing, which is sure to enhance security and efficiency.

The trust territory is independent in layers of networks. The theory presented in the paper is a general principle and could be applied into different layers and help to perform various tasks. In application layer, commercial websites could build there own trust territories and make trade safe. In networks layer, nodes select trusted nodes to transfer messages, which also need the support of trust territory theory.

This paper is organized as follows. Section 2 introduces trust theory. Section 3 addresses the concept of trust territory. Section 4 and 5 discuss the way to build trust territories. Finally the conclusions are summarized in the last section.

II. FOUNDATION OF TRUST THEORY

Before building trust territory of a node, we should review trust theory first.

A. The definition of trust

In information technology, trust can be defined as “the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context”[5]. This definition assumes that dependability covers reliability and timeliness [6].

B. Calculate trust value.

Calculating trust value is always the focus in trust theory and many abundant calculating approaches are presented in [2] and [4]. The basic rule to obtain trust value is by observations, which means past behavior determines the future. The way to get trust value is not discussed in the paper. We take trust value as a known quantity. Actually, trust value is also the function of actions, which is also ignored in the paper.
C. Subject and agent

We borrow two terms: “subject” and “agent” from [7]. When one node trusts the other node to perform an action, the first node is called the subject, the second node is called the agent.

D. Direct trust and trust recommendations

Trust value is divided into direct trust and trust recommendations. Direct trust is a parameter that indicates the subject could trust the agent to perform an action. Trust recommendation is a parameter that indicates the subject could adopt the recommendations from the agent. Direct trust and trust recommendation are used to construct different trust territory in the following sections. For simplicity, we say trust instead of direct trust.

III. TRUST TERRITORY

Trust Territory (TT) is a biggest set, which has a subset named as Compatibility Trust Territory (CTT), which also has a subset named as Equivalence Trust Territory (ETT). The relations among three sets are represented as (1).

\[ \text{ETT} \subseteq \text{CTT} \subseteq \text{TT} \]

Corresponding to three trust territories, there are three relations called as Trust Relation (TR), Compatibility Trust Relation (CTR) and Equivalence Trust Relation (ETR).

A. Trust Territory (TT)

Each node has Trust Territory, which is a set containing the identifications of its trusted nodes. The subject builds its own trust territory by trust values and the threshold. The simplest way to get TT is to set a threshold first and then the agent whose trust value after calculated is over threshold are inserted into Trust Territory of the subject.

B. Trust Relation (TR)

Let H be set containing only the subject.

\[ H = \{ \text{Subject} \} \]

TT is the trust territory of the subject. Trust Relation (TR) represents trust relationship among nodes in H \(\cup\) TT. If a ordered pair \(<a,b>\) \(\in\) TR, that means a trusts b. The binary relation TR in set H \(\cup\) TT is the reflexive closure of H \(\times\) TT indicated as (3).

\[ \text{TR} = (H \times TT) \cup \Delta = \{<a,b>|(a \in H) \land (b \in TT)\} \cup \{<a,a>|a \in (H \cup TT)\} \]

Here, “\(\Delta\)” is the symbol of conjunction. “\(\Delta\)” is the diagonal relation on H \(\cup\) TT.

It is obvious that Trust Relation is reflexive on set H \(\cup\) TT for node always trusts itself.

C. Compatibility Trust Territory (CTT)

Compatibility Trust Territory is the subset of Trust Territory. Assume “A” and “B” are nodes and “B” is in the trust territory of “A”, which means “A” trusts “B”. If “B” trusts “A”, “B” will be in Compatibility Trust Territory of “A”.

D. Compatibility Trust Relation (CTR)

CTR represents bidirectional trust relationship between subject and agent. CTR is a symmetric relation on set H \(\cup\) CTT(H is defined as above). CTR is the symmetric and reflexive closure of H \(\times\) CTT. The equation is as following.

\[ \text{CTR} = (H \times CTT) \cup (CTT \times H) \cup \Delta = \{<a,b>|a \in H \land b \in CTT\} \lor \{<a,a> | a \in CTT \land b \in H\} \]

Here, “\(\Delta\)” is the diagonal relation on H \(\cup\) CTT. “\(\lor\)” is the symbol of disjunction.

CTR is reflexive and symmetric, so it is a compatibility relation.

E. Equivalence Trust Territory (ETT)

Equivalence Trust Territory is the subset of CTT. Subject trust agents in Trust Territory (TT) will perform a certain action successfully; while subject believes agents in ETT could give right recommendations.

F. Equivalence Trust Relation (ETR)

ETR is an equivalence relation on H \(\cup\) ETT. A, B and C are the elements in H \(\cup\) ETT. If A trusts B and B trusts C, then A trusts C.

IV. BUILDING COMPATIBILITY TRUST TERRITORY

By calculating trust value and setting a threshold it is easy to get Trust Territory (TT), that is the subject knows who it should trust (direct trust). However, whether the trusted agent considers the subject credible is still unknown. Only nodes in Compatibility Trust Territory (CTT) have compatibility relations (reflexive and symmetric) with subject. Sometimes building compatibility trust territory is necessary and important for subject.

When we use trust theory to help routing, only trusted nodes are selected to transmit data and only routing request from trusted nodes will be taken into account. So it is not only useless but also harmful for the subject to send routing request to agent nodes that don’t trust it.

In electrical commerce, none wants to trade with someone who distrusts it. Building compatibility trust territory is a solution to build bidirectional trust relation.

A. Construct Trust Validation Message

By sending Trust Validation Message (TVM) to nodes in TT, the subject gets its CTT. In the paper, we try to ignore the differences among networks layers. When putting our trust territory theory into specific applications, message will be combined with corresponding protocols. Now we give the format of trust validation message in table 1.

TVMID is the identifier of Trust Validation Message, which indicates the function of the message. SubjectID is the identifier of the subject who sends TVM, while AgentID is the identifier of the agent who receives TVM.

B. Building CTT

A subject could send TVMs to any agent at anytime needed. The agent could also acknowledge to the subject by returning another TVM. If the agent doesn’t trust the subject, the TVM will be discarded. The subject will not wait for the return of the TVM. Whenever a subject receives a TVM, it will check if the agent shown in the TVM is in its TT. If yes, the agent will be put into the CTT; otherwise, the TVM will be ignored.
TABLE I. FORMAT OF TRUST VALIDATION MESSAGE

<table>
<thead>
<tr>
<th>TVMID</th>
<th>SubjectID</th>
<th>AgentID</th>
</tr>
</thead>
</table>

In order to cheat malicious nodes, a TVM may be sent to nodes outside the TT. Fig. 1 and Fig. 2 indicate the process to build CTT. A1, A2, A3 are three agents in the TT of the subject S. S receives TVMs from A1 and A3, so the CTT contains A1 and A3.

There is another way to extend CTT and will be discussed in the next section.

V. BUILDING EQUIVALENCE TRUST TERRITORY

Nodes in ETT could be trusted to give good recommendations. Two reasons encourage us to build ETT. Firstly, in some applications subject needs its trusted agents to provide recommendations the same as we need friends to give us advice. Secondly, building ETT is the way to extend trust territory.

In social society, we always hope to have more friends. Similarly, a bigger TT also provides more selections to make decision.

A. Building Initial ETT

Building initial ETT needs special trust values mentioned above, that is trust recommendations. How to get trust recommendation is discussed in [7]. Trust recommendations and a threshold could help the subject to construct initial ETT. The detail of the procedure is the same as to build TT.

B. Trust Graph

Graph could be used to represent trust relations. Take nodes as vertices. If A trusts B, a directed edge is drawn from A to B. So if B is in CTT of A, there will be a bidirectional edge between A and B. If node C is in ETT of A, we call C as “joint”. Each node has its own trust graph.

C. Extend Trust Graph

Each node will update TT by extending its trust graph. Trust graphs could be exchanged among trusted nodes. Periodically subject sends Trust Graph Request Messages (TGRMs) to all agents in its ETT. As defined above, only “joint” could receive TGRM if interception is not considered here. The destination “joint” (the agent) sends its trust graph to the source node (the subject) after receiving TGRM.

In subject’s view, all trust graphs from networks will be combined together to a new bigger trust graph, and then three trust sets may be enlarged. Assume G1 and G2 as two trust graphs. We combine G1 and G2 into a new trust graph G3.

1) Keep G1 and G2 unchanged.
2) Overlay joint with the same vertex (the same node).
3) The joint in G1 and G2 is also the joint in G3.

Following the above three principles we get a new graph G3. S is the subject in G1 and A is the vertex in G3. There are another three principles to extend three trust territories of G1.

1) If there is a path from S to A, the agent indicated as A is added into TT of the subject indicated as S.
2) If there is a path from S to A and from A to S, the agent indicated as A is added into CTT of the subject indicated as S.
3) If A is a joint and confirmed to be in the CTT of S, the agent indicated as A is added into ETT of the subject indicated as S.

Fig. 3, 4, 5 show the trust graphs of the subjects A, D and E. The three trust territories, TT, CTT and ETT are represented as Venn Diagrams. Double circles indicate the joint.

The subject A sends the TGRM (Trust Graph Request Message) to the agent D and E. D and E return their trust graphs to A. An enlarged trust graph is shown in Fig. 6. Fig. 7 shows A’s trust territories are extended.
VI. CONCLUSIONS

The typical ad hoc network application scenario is mobile and relatively dispersed network, so the security for ad hoc networks is a big challenge. Trust theory is one of solutions and has attracted attentions. Building trust territories provides a completely new view to trust theory. Trust territories could be constructed in all layers in the networks and applied into various applications. By communicating with nodes in trust territories, the security of ad hoc networks is enhanced.

REFERENCES