RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

Comparative Analysis of various Reputations based trust management system for Mobile Ad hoc Network

KEYWORDS: Ad hoc Network, attacks, malicious node.

Kajal S. Patel	Dr. J S Shah
Associate Professor (Computer Engineering) ,GEC, Rajkot, Gujarat.	Professor, LD Collage of Engineering, Ahmedabad

ABSTRACT Compared to wired networks, Ad hoc networks are more vulnerable to attacks. Security approaches used network like cryptographic techniques can not be directly used in ad hoc network due to limited resources of ad hoc nodes. Trust modeling and management can be used in ad hoc network to detect the abnormal activities and enhance security and other quality attributes of the system. Existing trust and reputation based routing protocols(TRIP, RIPSec,ARMAN, TRAVOS, RFSN, CONFIDANT etc) still vulnerable to one or more of following attacks. Like Playbook,Unfair rating, discrimination, collusion, proliferation, Reputation Lag exploitation, Re-entry, Sybil. Aim of this paper is to study and compare existing approaches used for ad hoc network which detects and avoids the malicious node and select best route for the packets and thus optimize performance of network. Also we want to identify the attacks which need more attention of the researchers..

I. INTRODUCTION

Social Trust is a belief that a person assumes that the other entity will behave in a specific way. Social trust can be cognitive and affective. Cognitive trust is influence by certain rules and regulation. Affective trust considers human emotions. It is very difficult to measure affective trust. According to researcher J sang there are two different types of trust. Evaluation Trust(reliability) ie. Trust is a belief (subjective probability) that an entity will perform in a way to bring expected benefits or not to do unexpected harm. Decision Trust ie. Trust is the extent to which one entity is willing to depend on others' decision and action accepting risk of negative outcome.

While considering digital world trust[1] can be represented as (1)Reputation which is a general standing of the community about an entity's trust worthiness based on the past behaviour, performance or quality of service of that entity in a specific context. (2) Rating that is Evaluation or assessment of something in terms of quality, quantity or both. And (3) Recommendation which is an opinion given by a trusted third party about an entity.

Trust Involves two entities – Trustor and Trustee. Trustor assess and make decisions for a given transaction and context while Trustee represents and put in a positive light on competence, honesty, reliability and quality of service.

Compared to wired networks, Ad hoc networks are more vulnerable to attacks due to

- the lack of a trusted centralized authority,
- easy eavesdropping because of shared wireless medium,
- dynamic network topology,
- low bandwidth,
- battery power and memory constraints of the mobile devices.

Security approaches used for wired network line cryptographic techniques can not be used due to limited resources (battery operated, low processing and memory capacity) of ad hoc nodes. Trust modeling and management can be used to detect the abnormal activities and enhance trustworthiness among nodes and thus enhance security and other quality attributes of the system. Many researcher have developed trust and reputation based routing protocols but still they are vulnerable to one or more of following attacks.

- Playbook
- Unfair rating
- discrimination
- collusion
- proliferation
- Reputation Lag exploitation
- Re-entry
- Sybil.

II. STATE OF ART

Researchers have designed and proposed various trust based routing protocol for ad hoc network. The recent protocols are TRIP, ARMAN, Provenance based trust model and Discount then filter based protocol.

A. TRIP

TRIP was proposed in " A trust and reputation infrastructure based proposal for vehicular ad hoc network" by Felix Gomez marno at science direct 2011.TRIP quickly detects malicious node who is spreading false or bogus messages throughout network. It classify each node into tree trust level represented with fuzzy sets. Reputation score computed from : direct experience, recommendations from neighbours and recommendation from central authorities.

$$Repi,j(t)=ai\ Repi,j(t-1)+ bi \sum Reck,j+ci\ RecRSU,j$$

ai , bi and ci are weight from direct previous experience of node.

Trust level represented as a fuzzy sets. "Trust", "No trust" and "+/-Trust". Each message has also severity levels: high, medium and low .TRIP is simple, light, fast and scalable trust and reputation scheme. Its simplicity make it vulnerable to malicious collective attacks.

B. ARMAN

This protocol was proposed in "Agent based reputation for mobile adhoc network" by Guy Gemkam, Djamel khadraoui etc. at PAAMS 2013, LNAI 7879, pp 122-132 2013 springer . The goals of this protocol was Enhance existing routing protocols in term of quality of service(packet delivery ratio), use similarity of belief to deal with unfair ratings and to reduce uncertainty while integration of second hand information Dempster Shafer theory is used. We will discuss the similarity view with the help of example.Given two nodes A and B. Let A trustor and B be recommender in neighbour of A. let {C,D..} nodes A and B communicated with in past. similarity view is calculated,

$$sim(A,B)= 1-dis(A,B)$$

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

dis(A,B)=sqrt(∑(DRA,i-DRB,i)2)

where iϵ{c,D…}

The observation from recommender B is accepted only if similarity view with A is greater than threshold value otherwise rejected.

A 's belief on C and be computed TA,C= DRA,C+ recommendation from neighbours(indirect trust) Let B1 and B2 provides observation, these observation are combine using Dempster shafer sum. let frame of discernment is f= {U, T} , power set ={{U},{T},{U,T},ø}, a trust function bel(ø)=0 and bel(f)=1 If B1 and B2 are uncertain about C, their trust belief is calculated as follows,

belB1(f)=0.4 belB2(f)=0.3

belB1({T})=0.6 belB2({T})=0.7

belA,C=0.6*0.7=0.42

This protocol is vulnerable to proliferation and Reputation Lag Exploitation attack.

C. Provenance based trust model

This protocol is designed for DTN(Delay Tolerant Network). DTNare used in military where end to end connectivity of network is not guaranteed due to frequent disconnection or delay.Provenance mean history of ownership of valued object. The proposed provenance based trust model has following features: reduce communication overhead by not incurring extra communication overhead for trust evolution purpose addition to message delivery, use reward and penalty strategy, consider availability, integrity and competence and SPN is used to identify optimal trust threshold to max accuracy and min communication overhead. The authors check robustness of this scheme against following attacks:Fake identity, Good or Bad mouthing, Message Modification, Packet dropping.

D. Discount then filter based protocol

The Discount then filter based approach was introduced in "Robustness of trust models and combinations for handling unfair ratings" by Lizi Zhang, Siwei Jiang and Wee Keong Ng at IFIPTM 2012, IFIP ACT 374, pp 36-51, 2012. They have discussed various attacks due to unfair ratings in various trust based routing like Constant attack, Camouflage attack, Whitewashing attack, Sybil attack, Sybil Camouflage attack, and Sybil Whitewashing attack. They also have analysed the Beta Reputation System, iCLUB , TRAVOS, and Personalised scheme for handling unfair rating. Authors also categorised BRS and iClub as filter based and TRAVOS and Personalised as Discount based model. After comparing the above mentioned trust model authors concluded that Discount –then- Filter scheme is robust against all investigated attacks except TRAVOS+BRS. But still there are attacks like discrimination, proliferation etc not addressed by authors

III. COMPARATIVE ANALYSIS OF EXISTING PROTOCOLS

The Result of comparative analysis of all the above explained models for various attacks on trust/reputation based routing is shown in following table.

TABLE I: THE COMPARISON OF EXISTING TRUST MODELS

Trust model	Playbook	Unfair Rating	Discrimination	Collision
TRIP	Yes	Yes	Yes	NO
ARMAN	Yes	Yes	Yes	Yes
Provenance based trust model	NO	Yes	Yes	NO
Discount then filter based trust model	Yes	Yes	NO	Yes

Trust model	Proliferation	Reputaion Lag exploitation	Re entry	Sybil
TRIP	NO	NO	partial	NO
ARMAN	NO	NO	Yes	yes
Provenance based trust model	NO	NO	Yes	NO
Discount then filter based trust model	NO	NO	Yes	Yes

IV. CONCLUSION

After comparing the above mentioned schemes we have concluded that all model consider the attacks which intentionally drop the packets or alter/modify the packets. They have not consider delay in packet forwarding . We will consider this delay in our proposed model to calculate the trust or reputation values.

REFERENCE

1) Co- evolving trust mechanism for Catering User Behaviour by Tanja Azserska at IFIPTM 2012, IFIP ACT 374, pp 1-16, 2012. | 2) Rubustness of trust models and combinations for handling unfair ratings by Lizi Zhang, Siwei Jiang and Wee Keong Ng at IFIPTM 2012, IFIP ACT 374, pp 36-51, 2012. | 3) Dynamic Trust Models for ubiquitous computing environment by colin english, paddy Nixon, Sotirios Terzis, Andrew McGettrick, Helen Lowe at EU FET project GLOSS: Global samrt spaces 2009. | 4) A Provenance based trust model for delay tolerant networks by Jin Hee cho, Moonjeong Chang, Ing Ray Chen and Ananthram Swami at IFIPTM 2012, IFIP ACT 374, pp 52-67, 2012 | 5) Reputation Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review by Hani Alzaid, Manal Alfaraj, Sebastian Ries, Audun Josang, Muneera Albabtain, Alhanof Abuhaimed at IFIPTM 2013, IFIP ACT 401, pp 62-82, 2013 | 6)Challenges for Robust of Trust and Reputation Systems by Audun Jøsang and Jennifer Golbeck. Proceedings of the 5th International Workshop on Security and Trust Management (STM 2009). Saint Malo, France, September 2009.