International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Trust Based Routing Protocols for Mobile Ad Hoc Networks: A Survey

Saurin Choksi[1], Nikhil N. Gondaliya[2]
Student Information Technology[1],Head of Information Technology Department[2],
G.H.Patel college of Engineering and Technology, .V.Nagar, Anand Gujarat-India [1, 2],
Email: choksisaurin@gmail.com[1], nikhilgondaliya@gcet.ac.in[2]

Abstract – Mobile Ad-hoc networks (MANETs) have various characteristics like mobility, infrastructure less, spontaneously created and can be established in any environment without pre-existing infrastructure with ease of deployment. Due to these characteristics of MANETs they can be used for various applications. However to use MANETS in commercial purpose they must be secured from malicious attackers. Providing security to MANETs is difficult due to vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. Various trust based routing protocols are discovered to provide security and better throughput by detecting and eliminating malicious nodes from the network but trust computation is a highly challenging task due to independent characteristics of MANETs. In this paper we have presented a detailed survey on various trust based routing protocols for MANETs, how they have achieved security against malicious attacks and also discuss the future research directions for finding trust.

Index Terms- MANETs, trust, trustor, AODV,QOS.

1. INTRODUCTION

The mobile ad hoc networks (MANETs) are complex wireless networks which have little or no existing network infrastructure. These networks can be established in a spontaneous manner allowing organizations and network members to work together and communicate, without a fixed communication structure. The mobility, spontaneity and ad hoc nature of these networks makes them optimal solutions for disaster area communication and tactical military networks. Due to recent wireless technology advances, mobile devices are equipped with sufficient resources to realize implementation of these dynamic communication networks [1]. But Due to this characteristics of manets there are some challenges like Dynamic architecture, self organized nature, No prior relationship, Multi-hop communication channel, mobility, security, resource limitations and physical vulnerability [1]. From these challenges our focus is on security of mobile ad hoc networks.

Security in mobile ad hoc networks is difficult to achieve, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. Earlier studies on mobile ad hoc networks (MANETs) aimed at proposing protocols for some fundamental problems, such as routing, and tried to cope with the challenges imposed by the new environment. These protocols, however, fully trust all nodes and do not consider the security aspect. They are consequently vulnerable to attacks and misbehaviour [2].

There are different types of attacks can be considered for network security like insider and outsider attacks, attacks on different layers and active and passive attacks can be possible[3]. The different types of attacks also can be possible on manets like Warmhole attack, Blackhole attack , Grayhole attack , Rushing attack , Dropping Data packets attack and many more [2].

To provide solutions against these types of various attacks different solution has been discovered until now like using security key management, Intrusion Detection System, trust management and many more. Out of them our focus is on analysis of different trust based solutions for providing security against different types of attacks.

2. TRUST: CONCEPT, PROPERTIES, COMPUTATION AND METRICS

Trust in manet can be derived by observing the behaviour of other nodes. Different methodologies are used to observe behaviour to take the evidence and to calculate the trust for particular node. So in this section the basic concept of trust, properties of it and how the trust can be computed using different metrics is described.

A. Trust Concept

Trust is an important aspect of mobile ad hoc networks. It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques suited for other networks. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the

quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node [4].

So the definition of the trust can be given like: *The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context.* Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/behaviour. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted by the given node [4].

B: Trust Properties

There are many properties of trust have been derived until now and they are Asymmetric, Transitivity and Composability, dynamic,subjective. [4][5]. Asymmetric means 2 nodes can have different trust value for each other. Transitivity means trust value can be propagated through trusted nodes. Composability means the trusted route can be discovered by composing trust value of each node in a path. Dynamic means trust for particular nodes can be changed in a time. Subjective means a trustor node may determine a different level of trust against the same trustee node due to different experiences with the node derived from a dynamically changing network topology.

C: Trust Computation

Trust can be computed by using 3 ways.(1)Direct(sensing the neighbour).(2)Indirect Trust(based on recommendation of neighbour nodes)(3)Hybrid Trust [5].In Direct Trust Every node measures the trust degree of the other nodes by analyzing their behaviour at different time. For example node a analyze the behaviour of node b using different parameters and assign some trust value and based on that trust value the node can conclude whether to trust on that node for forwarding the packets. The indirect trust is based on the recommendation of other nodes for the particular suspect node. For example node a can get the recommendation of node b from trusted node c or may be from many other nodes and based on averaging the total weight the trust weight can be derived. So in this way how recommendation of trust can be used to find the trust value of the suspect node. In hybrid trust the total trust value of the node can be derived by combining the both direct and indirect trust. For example node a can evaluate weight of trust b by combining both its own evaluation of trust and also recommendation of trust for node b from other nodes. The recommendation can be computed using different techniques like simple average, greedy approach and weighted average also. So different techniques can be used for different purposes.

D. Trust Metrics

The trust metrics that are used in different management schemes are like over heads, goodput, packet dropping rate, packet delivery ratio and delay. Route usage (refers to the number of routes selected particularly when the purpose is for secure routing). "Trust level" is a recently used system metric. The trust value, trustworthiness, opinion values about other nodes, and trust level per session and other metrics that consider system tolerance based on incorrect reputation threshold, availability, convergence time to reach steady state in trustworthiness of all participating nodes, and percentage of malicious nodes.[5]

We can say that different trust parameters can be used for different purposes like to improve throughput and performance packet dropping or forwarding ratio can be used and to improve quality of services of manets delays or overheads can be used as a trust parameters.

In the next section we will see different trust based routing schemes that solve different security issues for manets.

3. TRUST BASED ROUTING PROTOCOLS IN MANET

Different trust based schemes are discovered to provide security to manets by using different trust parameters and by considering different attacks.

D. Umohoza *et al* [6] has proposed a trust based scheme in which trust can be computed based on QoS parameters. Probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays are used to estimate and update trust. Functions which facilitate this are provided and evaluated. It has been shown that only two end nodes need to be involved and thereby achieve reduced overhead. The framework proposed is applicable and useful to estimate trust in covert unobservable and anonymous communications. But the limitation is that to measure all the probability of different parameters can be tedious task

Pedro B. Velloso *et al* [7] has proposed the the trust based scheme based on based on previous individual experiences and on the recommendations of others. The Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbours is presented. The nodes only need to keep and exchange trust information about nodes within the radio range. The proposal scales well for large networks while still reducing the number of exchanged messages and therefore the energy consumption. In addition, the effect of colluding attacks composed of liars is mitigated in the network but the limitations is that this framework takes time to identify which node is more trusted and which one is not.

Jian Wang *et al* [8] have proposed different trust computation techniques instead of packet dropping ratio. In this technique the similarity degree between nodes is used as a trust metrics like velocity, moving directions, and affiliated organization and it gives good performance in mobile conditions but the limitations is that it is complicated to select the similarity attributes for computations of trust as far as the security is concern.

Bo Wang *et al* [9] has applied the trust based framework on minimum cost opportunistic routing to provide the security to same. In order to remove the malicious behaviours, this method incorporates the concept of trust to Ad hoc networks, build a simple trust model to evaluate neighbours' forwarding behaviour and apply this model to opportunistic routing for Ad hoc networks. It uses both direct and indirect trust for computation but limitations is more computation overhead and quality of service should be considered for better performance.

Zhi Li *et al* [10] has proposed the trust based mechanism using autoregression function. This mechanism used 2 models, Autoregressive (AR) model and Autoregressive with exogenous inputs (ARX) model. According to this mechanism, a node periodically measures the packet forwarding ratio of its every neighbour as the trust observation about that neighbour using packet delivery ratio. The node has such a time series for each neighbour. By applying an autoregression model to these time series, it predicts the neighbour's future packet forwarding ratios as their trust estimates, which is used to make intelligent routing decisions. With an AR model , the node only uses its own observations for prediction; with an ARX model, it will also take into account recommendations from other neighbours but the limitations is that it will take extra storage space to store and secure recommendations.

Hui Xia *et al* [11] has proposed a trust based technique in which trust is computed based on historical observation and also future prediction using fuzzy logic. This method also integrated the proposed trust predication model into the Source Routing protocol. This on-demand trust-based unicast routing protocol for MANETs, uses packet delivery ratio to choose the shortest route that meets the security requirement of data packets transmission but the limitations is that due to more computation for finding the trusted route the end to end delay might be compromised.

Jin-Hee Cho *et al* [12] has proposed a trust based routing protocol in which trust is identified using sochestic petrinet model and new trust metrics are identified as social trust and qos trust. In social trust they have considered honesty and closeness and for qos trust they have considered energy level and degree of cooperations. So by using these trust metrics the trust weights are computed and routing is done on the basis of that. The limitations of this proposed routing protocol is that it has more computation task as global trust is considered and qos parameters like delay should be considered for better performance.

R. Datta *et al* [13] has proposed a light-weight trust-based routing protocol. It is light-weight in the sense that the intrusion detection system (IDS) used for estimating the trust that one node has for another, consumes limited computational resource and uses packet delivery ratio as a trust metrics. Moreover, it uses only local information thereby ensuring scalability. This mechanism takes care of two kinds of attacks, the blackhole attack and the grayhole attack and the authors have used AODV as the base routing protocol. The limitations of proposed scheme is it vulnerable to false recommendation attack and it should be eliminated.

Bo Wang *et al* [14] has proposed a trust based routing scheme in which with packet delivery ratio as a trust metrics the link quality (ETX metrics) is considered to provide QoS guarantee. So the proposed method ensures the forwarding of packets through the trusted and least link delay routes only by monitoring the behaviour of neighbouring nodes and meeting the QoS constraint accordingly. But the limitation is that it is vulnerable to false recommendation attack and also ETX metrics does not provide the better qos guaranty.

Table I summarizes trust management schemes surveyed in this section. It explains how trust evidence is collected and performance metrics used to evaluate various trust management schemes.

Author and year	Trust type and Method used	Trust Metrics	Attack Considered	Advantages	Limitations
D. Umohoza et al 2007 [6]	Direct trust Using qos parameters	Probabilities of transit time variation, deleted,multiplied and inserted packets, processing delays	Not Considered	Efficient by measuring traffic analysis	Measuring probabilities for all the parameters is complicated task.
Pedro B. Velloso et al 2011 [7]	Hybrid trust using Recommendation and Based on Maturity	Packet Farwarding ratio	Slander Attack, Changing Behaviour Attack	Low Resource Computation and Eliminate False Recommendation.	Due to maturity it takes time to identify the malicious nodes.
Jian Wang et al 2011 [8]	Hybrid trust using Similarity Degree	velocity, moving directions, and affiliated organization	Black hole, Slander Attack, Changing Behaviour Attack	It gives Better performance against original DSR.	Complexity in Choosing similarity attributes as far as security is concern.
Bo Wang et al 2011 [9]	Hybrid trust on minimum cost opportunistic routing	Neighbour forwarding ration	Not Considered	It is Efficient in resisting malicious attacks, cost of routing and throughput	It has more control overhead, and Qos assurance can be implemented for better performance
Zhi Li et al 2011 [10]	Hybrid trust Using autoregresion function	Packet Forwarding Ratio	Not Considered	Accurate and gives improvement to greedy algorithm.	It requires extra local space for storing recommendations.
Hui Xia et al 2012 [11]	Hybrid trust using Historical & Prediction using fuzzy logic	Packet forwarding Ratio	Black hole, Gray hole	More reliable route is obtained and secure against various attacks.	More computation overhead and qos routing can be applied.
Jin-Hee Cho *et al* 2011 [12]	Global trust using Social trust and qos trust using SPN model	Honest, Closeness ,energy level and degree of cooperation	Not Considered	Trusted route can be discovered as trust chain is used for computing trust.	It has more overhead due to computing global trust.
R. Datta et al 2012 [13]	Hybrid Trust by averaging recommendation.	Packet Forwarding Ratio	Black hole, Grey hole	Low Traffic overhead and Low computation cost	Mobility issues and False Recommendation should be eliminated
Bo Wang et al 2013 [14]	Hybrid trust and Link quality is combined for computing trust.	Packet Forwarding Ratio and ETX metrics is used.	Black hole, Gray hole	prevent attacks from security nodes and improve the security and qos	False Recommendation should be eliminated and ETX is not as much accurate.

Table I Survey on existing trust based routing protocols

4. CONCLUSION

The trust schemes presented in this paper cover a wide range of application and are based on many different types of mechanisms. There is no single solution that will be suitable in all contexts and applications. While designing a new trust system, it is necessary to consider the constraints and the type of information that can be used as input by the network. A general observation is that so far, the existing research work and proposals lack completeness. So to provide a better trust based routing scheme a researcher should analyse the limitations of the different trust based mechanism based on considering different attacks and also the throughput of the network and try to investigate for a hybrid trust metrics and improving security against different attacks and also to improve overall performance of the network.

ACKNOWLEDGEMENT

My Sincere thanks to my guide Prof. Nikhil N Gondaliya, for providing me an opportunity to do my research work. I express my thanks to my Institution namely G. H. Patel College of Engineering and Technology for providing me with a good environment and facilities like Internet, books, computers and all that as my source to complete this research work. My heart-felt thanks to my family, friends and colleagues who have helped me for the completion of this work.

REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[2] Djmel djenouri and lyes khelladi, "A survey of security issues in mobile ad hoc and sensor networks", IEEE communications surveys & tutorials , fourth quarter 2005

[3] Stallings W.,"Cryptography and Network Security: Principles and Practices",Prentice Hall, 2003.

[4] Kannan Govindan, Prasant Mohapatra," Trust computations and trust dynamics in mobile ad hoc networks: a survey", IEEE Communications Surveys and Tutorials 14 (2) (2012) 279–298.

[5] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, "A survey on trust management for mobile ad hoc networks", IEEE Communications Surveys and Tutorials 13 (4) (2011) 562–583. Fourth Quarter.

[6] D. Umuhoza, J.I. Agbinya, C.W. Omlin ,"Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms", AusWireless 2007, IEEE

[7] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model", IEEE Transactions on Network and Service Management 7 (3) (2010) 172–185.

[8] Jian Wang, Yanheng Liu, Yu Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", Journal of Network and Computer Applications 34 (4) (2011) 1138–1149

[9] Bo Wang, Chuanhe Huang, Layuan Li, et al., "Trust-based minimum cost opportunistic routing for Ad hoc networks", Journal of Systems and Software 84 (12) (2011) 2107–2122

[10] Zhi Li, Xu Li, V. Narasimhan, "Autoregression models for trust management in wireless ad hoc networks", in: IEEE Globecom, 2011, Kathmandu, Nepal.

[11] Hui Xia, Zhiping Jia , Xin Li, Lei Ju, Edwin H.-M. Sha,"Trust prediction and trust-based source routing in mobile ad hoc networks", Elsevier,2012

[12] Modeling and analysis of trust management with trust chain optimization in mobile adhoc networks Jin-Hee Cho , AnanthramSwami , Ing-RayChen , Journal of Network and Computer Applications ,2011

[13] N. Marchang, R. Datta,"Light-weight trust-based routing protocol for mobile ad hoc networks", IET Information Security 6 (2) (2012) 77–83.

[14] Bo Wang, Xunxun Chen, Weiling Chang,"A light-weight trust-based QoS routing algorithm for ad hoc networks", Elsevier,2013.