Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Trust Based Routing Protocols in MANET

Mrs. S. Geetha
Department of MCA
BIT Campus, Anna University Chennai
Chennai, India

Dr. G. Geetha Ramani
Department of Mathematics
BIT Campus, Anna University Chennai
Chennai, India

Abstract - A Mobile adhoc network is a self-organized multi hop system comprised by multiple mobile wireless nodes with peer-to-peer relationship and without any fixed infrastructure. It is vulnerable to attacks from malicious nodes since there is no centralized administration and security and hence the qualities of overall networks are also easily affected. Trust is an important aspect of mobile ad-hoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. In this connection, a lot of research has been going on and a number of trust based routing protocols have been proposed in the literature. This paper does a detailed survey on the trust based routing protocols namely AODV, DSR, OLSR, TORA, DSDV and TRAP. This paper also elucidates the comparison between these protocols in a table1.

Keywords: Trust, MANET, Multihop, AODV, DSR, OLSR, TRAP, TORA, DSDV

I. INTRODUCTION

Mobile ad hoc Networks are dynamically configured, multi hop wireless networks characterized by absence of any infrastructure, dynamic topology and wireless links. MANET composed only of nodes and these nodes do not have fixed infrastructure or any centralized controller such as access point or server to determine the route of the paths. Thus each node in an ad hoc network has to rely on each other in order to forward packets and there is a need to use a specific cooperation mechanism to forward packet from hop to hop before it reaches a required destination by using routing protocol.

As nodes may not be aware of to which nodes it is connected with or which nodes connected to them. Therefore access to resources or information can be shared among both trusted and non trusted nodes. The inherent freedom in self organized mobile ad hoc networks introduce challenges for trust management. when nodes do not have any prior knowledge of each other. Hence, to assure that access to resources is given only to trusted nodes, the trustworthiness among anonymous nodes needs to be formalized.

Trust is an important aspect of mobile ad-hoc networks (MANETs). 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. In this work detailed survey on various trust computing approaches that are geared towards MANETs has been done.

The rest of this paper is organized as follows. In Section 2, this paper presents a trust definition and trust mechanism. Then, Section 3 describes the brief overview of the various trust based routing protocols and the comparison between these protocols. Section 4 gives conclusion of this work.

II. TRUST DEFINITION AND TRUST MECHANISM

A. TRUST DEFINITION

A standard definition considers trust to be a measure of subjective belief that one person or party uses to assess the chance another can perform a good action before the chance presents itself to observe whether or not that activity has occurred. Once an individual is taken into account trustworthy, it's meant that there's a high chance that the actions they're expected to perform are done in a way that's favorable to the trusted.

In MANET trust will be outlined as a level of belief in line with the behavior of nodes the chance value of trust variable from zero to one wherever zero represents DISTRUST and one represents TRUST. Providing trust model in ad hoc networks is important as a result of it gains higher security level and improves efficiency within the network.

The dynamics of this has contributed to three main analysis areas within the field of Trust Management for distributed ad-hoc networks. This includes work targeting Trust Propagation, Trust Aggregation and Trust Prediction. Once developing any sort of Trust Management scheme for a MANET, the calculations of following values must be done accurately:

- Trusting Accuracy: The trust algorithms must effectively calculate trust with preciseness even in the presence of malicious nodes.

• Detection of malicious nodes: The aggregation operations are used to detect the malicious node and should be propagated to the neighboring nodes about its suspicious activity.

‘‘The notion of trust is fundamental for understanding the interactions between devices such as human beings, organizations, nations and others. The fact that a node A trusts a node B in some respect, informally, means that A believes that B will behave in a certain way and will perform some action under certain specific circumstances’’

B. TRUST MECHANISM

Trust Mechanism is introduced in the protocols to provide security in MANET. Trust is a value that is calculated in the basis of nodes action when needed. Trust is introduced to prevent from various attacks like worm-hole, black hole, Dos, Selfish attackes etc. Trust can be implemented in various ways such as reputation, subjective logic from opinion of needs etc as there are no particular definition of trust. According to trust has following properties.

- Context Dependance : In some specific context trust relationships are applicable.
- Function of Uncertainty: Trust depends on the uncertainty of nodes action. It gives the probability of action performed by a node.
- Quantitative value: Trust can be assigned any type of numeric values discrete or continuous.
- Asymmetric Relationship: Trust relationship is asymmetric in nature. If node A trusts B and node B trust C that does not mean that A trusts C.

C. TRUST and SECURITY

Trust and security should go hand in hand. The level of trust has an impact on the level of security. The wireless networks involve various types of security domains and security implementation mechanisms. A trust relationship which considers the heterogeneousness of these networks security procedures is essential. This can be accomplished by specifying the levels of security requirements and security mechanisms such as encryption, digital signature, authentication at the boundaries of each integrated networks. In other words, each of the integrated networks should contain their own security requirements along with the levels of trust (and even reputation) they are willing to provide to other networks or nodes.

III. TRUST PROTOCOLS DESCRIPTION

A. TRUST DSR

TDSR [4] reduces the number of packets dropped by node and it works on the basis of positive or negative acknowledgement after a packet transmission. The authors use a trusted route for data transmission. It may be used for better performance of the network. The trust of a node is decided on the basis of all the successful and unsuccessful transmission done by a node. This is evaluated by counting the number of ACK (Positive acknowledgement) and NACK (Negative acknowledgement) sent by a node. TDSR finds the foremost secure route from source to destination in a network. Protocol projected can facilitate in forming, updating and maintaining the trust within the network. It helps in selecting the foremost reliable route within the network supported by the trust values of the nodes lying in a route. A node in the network maintains a table with a record of all its neighbors with their trust values which is updated periodically. The trust of a node in the network is evaluated based on its performance in the network. If a node successfully transmits a packet it sends a positive acknowledgement to the sender and results in upgrading its trust value. Dropping of a packet results in negative acknowledgement which results in reduction of the trust value of a node. The table storing the trust value of all neighbors is broadcasted periodically so that the information about the most trusted node is known to all. Trust value of a node helps in choosing the most trusted route from source to destination. This method evaluates trust of all the routes from source to destination based on the trust values of the intermediate nodes in the forward path and then chooses the route with the minimum trust worth (greater or equal to some trust threshold value).

B. TRUST BASED OLSR

In TOLSR [5], trust-based analysis of the OLSR protocol using trust specification language is presented and the authors show how trust based reasoning can allow each node to evaluate the behavior of the other nodes. They have presented a trust-based solution for securing the OLSR Ad hoc routing protocol in three steps. The first step was the analysis of the implicit trust relations in OLSR. This analysis highlights the possible measures to make OLSR more reliable by exploiting the operations and information already existing in the protocol. To detect misbehaving nodes, they have developed in the second step, trust-based reasoning by correlating information provided in the OLSR messages received from the network. The integration of this reasoning allows each node to check the consistency of the behavior of other nodes and validate trust relationships established implicitly. Finally, the third step complements the second by offering two complementary solutions: prevention to resolve certain vulnerabilities of OLSR protocol, and countermeasures to stop and isolate malicious nodes. These proposals correspond to the trust reasoning that has been done by each node. Simulation results illustrate the effectiveness of trust-based reasoning and countermeasures to stop and isolate misbehaving nodes.

After the detection of misbehaving nodes, the solutions of prevention and countermeasures to resolve the situations of inconsistency, and counter the malicious nodes are provided. How a node can detect misbehavoring nodes by reasoning about information received from the network is investigated. Anomaly detection includes the consistency verification in OLSR messages (TC and HELLO) and trust-based reasoning that can be performed by each node in the network.

Although it is a continuous process, the detection must progress from the reception of the link discovery messages to the construction of the routing table, giving the particular evolution of trust among nodes during these operations. The authors address the countermeasure concerns in the basic operations in OLSR (neighborhood discovery and MPR selection) and the distribution of information about trust relations and attack detection to alert the other nodes. For this, the time-stamp mechanism proposed by SOLS and the provable identity mechanism presented previously, are set up respectively to ensure the freshness and authentication of messages.

C. TRUST TORA

Trust TORA[6] proposed a mechanism especially viable for ad-hoc networks that can be created on the fly without a formal trust infrastructure including Certification Authorities and Key Distribution Systems and proposed a unique method for exchanging and establishing trust in ad-hoc networks that are void of a trusted third party. For that, an effort-return based trust model in a decentralized manner so as to create a self-organized reliable network. Based upon functionality, the trust model can be divided into the following three components: Trust agent, Reputation agent and the Combiner. The Trust agent extracts trust information from the events that are directly experienced by a node. The Reputation agent shares trust information with other nodes in the network. The Combiner calculates the total trust in a node from the information that it receives from the Trust and Reputation agents. Each category in TORA is represented by one or more types of events. Events are logged into tables based upon their success or failure rate. These events are then normalized to generate information, which can be used by the trust agent. The majority of events that are experienced by a node take place within the vicinity of its direct neighbors. This helps to institute Direct Trust relationships among the neighbors.

On the other hand, very few events are directly experienced between nodes that are more than one hop away. To get an extended evaluation of the trust arrangement, the reputation of nodes has to be taken into consideration while computing trust in nodes. The Trust Agent, Reputation Agent and the Combiner maintain and update the Direct, Reputation and Derived/Aggregate Trust values depending upon the frequency of events and severity of the situation. The trust values further refine as the trust model matures with passage of time. These values can be applied to different services under diverse scenarios. Some of the possible usages are Route Discovery, Route Maintenance, Security and Quality of Service. These trust reputations provide the nodes with vital information regarding trust levels of other nodes beyond a single hop. However, malicious nodes may exploit this mechanism of trust exchange by overwhelming other nodes with a large number of fabricated requests for reputation. In order to suppress the rate of fictitious requests, Hash Cash tokens that inherently limit the number of recommendation request packets are employed, which can be generated over a certain interval.

D. TRUST AODV

TAODV [7], is a trusted routing protocol using trusted frame works and intrusion detection system for MANET. Trust combination algorithms and trust mapping functions are provided in this model, where the former can aggregate different opinions together to get a new recommendation. Based on this trust model, to design the trusted routing protocols for MANET called TAODV on top of Ad Hoc On-demand Distance Vector (AODV) routing protocol, is propose by the authors. The routing table and the routing messages of ADOV with trust information which can be updated directly through monitoring in the neighborhood are used here. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, the authors combine the recommended opinions together and make a routing judgment based on each element of the new opinion. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedure can be guaranteed as well. In this work, they implement the security and selfishness issues of wireless networks, either in non-cooperative form or in cooperative form. Their results show that the cumulative utilities of cooperative nodes are increased steadily and the selfish nodes cannot get more utilities by behaving selfishly than cooperatively

In this work, for some assumptions are made to establish the network model of Trust AODV (TAODV). It also argues why the authors shows security solution on routing protocol in the network layer instead of link layer. Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. In TAODV, it is assumed that the system is equipped with some monitoring mechanisms or intrusion detection units either in the network layer or in the application layer so that one node can observe the behaviors of its one-hop neighbors. In the network layer, a new node model is designed as the basis of the trust model. Some new fields are added into a node’s routing table to store its opinion about other nodes’ trustworthiness and to record the positive and negative evidences when it performs routing procedures with others. By embedding the trust model into the routing layer of MANET, the consumption of time can be saved without the trouble of maintaining the expire time, valid state, etc.,

E.TRUST DSDV

TDSDV[8], proposed Trusted Destination Sequenced Distance Vector (TDSDV) Routing Protocol for MANET is a proactive secured routing protocol. It gains some of the inherent qualities of the distance vector algorithm. In such kind of proactive routing protocols, each node repeatedly maintains state-of-the-art routes to every other node in the network, Routing information at regular intervals are transmitted throughout the network. In order to preserve routing table stability, when the route discovery process is initiated, the two state-of-the art estimations such as bandwidth and variance residual energy will be calculated. The routing table is updated at every node by discovering the variation in routing knowledge about all the existing destinations with the number of nodes to the destination.

When the attacker tries to impersonate as intermediate node this TDSDV protocol will recognize the intruder using Intruder Detection Methodology, and redirect the path to the destination. In addition, to offer loop freedom, this protocol TDSDV uses succession count, which is offered by the destination node. When a route has already existed before traffic arrives, transmission takes place without any delay. Else, traffic packets must wait in queue till the node gets routing information equivalent to its destination. In case of highly dynamic network topology, the proactive schemes need a noteworthy quantity of resources to maintain routing information up-to-date and reliable.

F. TARP

TARP [9], is a Trust Aware Routing Protocol for secure trusted routing in mobile ad hoc network. This protocol is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes and determines the route based on these attributes. The security attributes considered in computing the trust level of a node in a given route include: Software configuration, hardware configuration, battery power, credit history, exposure and organizational hierarchy. Each node evaluates the trust level of its neighbors based on the above attributes and includes it in computing the next hop node in the overall shortest route computations. This protocol uses two important attributes like battery power and software configuration.

In Wireless networks, the battery power with which nodes operate is a limited resource. Each node uses its power to not only send and receive, but also to behave as a router by forwarding routing messages and updates. The cryptographic techniques that provide security are computationally intensive, further increase the power consumption of a node. The power is an important attributes for evaluating the trust level of a node and the Software configuration includes the encryption ability of a node. To satisfy CAI (Confidentiality, Availability and Integrity), different cryptographic mechanisms have been proposed. Some are based on symmetric encryption and others on asymmetric encryption. Each node is given either a shared secret key or public key pair depending on the type of cryptographic mechanisms.

A secure route between a source and destination is established based on a confidence level prescribed by a user or application in terms of these attributes. It requires a robust and adaptive trust routing algorithm that reacts quickly and effectively to the dynamics of the network. It finds the shortest path to the destination. TARP is able to improve security and at the same time reduce the total routing traffic sent and received in the network by directing the traffic based on the requested sender attributes.

IV. CONCLUSIONS

The level of trust has an impact on the level of security. The wireless networks involve various types of security domains and security implementation mechanisms. A trust relationship which considers the heterogeneousness of these networks security procedures is essential. 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. A lot of trust based routing protocols have been found in the literature. Each trust based protocol finds the trusted path by using a different mechanism and the usability of any protocol is mainly based upon the context in which it is being used.

REFERENCES

[1] Eissa, T., Abdul Razak, S., Khokhar, R. H., & Samian, N. (2013). Trust-based routing mechanism in MANET: Design and implementation. Mobile Networks and Applications, 18(5), 666-677.

[2] Meka, K., Mohit Virendra, and Shambhu Upadhyaya. "Trust based routing decisions in mobile ad-hoc networks." Proceedings of the Workshop on Secure Knowledge Management (SKM 2006). 2006.

[3] Pirzada, Asad Amir, and Chris McDonald. "Establishing trust in pure ad-hoc networks." Proceedings of the 27th Australasian conference on Computer science-Volume 26. Australian Computer Society, Inc., 2004.

[4] Khatri, Pallavi. "TDSR: Trust based DSR Routing Protocol for Securing MANET." INTERNATIONAL JOURNAL OF NETWORKING AND PARALLEL COMPUTING 1.3 (2013): 42-48.

[5] Asma Adnane, Christophe Bidan , Rafael Timóteo de Sousa Júnior “Trust-based security for the OLSR routing protocol” Elsevier April 2013.

[6] Pirzada, Asad Amir, AmitavaDatta, and Chris McDonald. "Trustworthy Routing with the TORA Protocol."Proceedings of the AusCERT Asia Pacific Information Technology Security Conference. 2004.

[7] Pankaj Sharma, et al. “ Trust Bsed Secure AODV In MANET” Journal of Global Research in Computer Science” Vol3. No6, June 2012.

[8] MohdZamirArif, et al. “ Trusted Destination Sequenced Distance Vector Routing Protocol for Mobile Ad-hoc Network” International Journal of Computer Applications September 2013.

[9] Abusalah, Loay, et al. "TARP: trust-aware routing protocol." Proceedings of the 2006 international conference on Wireless communications and mobile computing.ACM, 2006.

Table1. Summary Report for trust based routing protocols

S. No	Authors & Year	Context in use	Mechanism	Advantages	Limitations
1.	Pankaj Sharma, et al & 2012	TAODV	Intrusion Detection Algorithm	Trust model is built into the routing layer of MANET, it can save consuming time without the trouble of maintaining the expire time, valid state etc.	It cannot synchronize the trust level setting on different nodes when multiple paths cross with each other.
2	] Khatri, Pallavi & 2013	TDSR	Trust is evaluated based on performance sending acknowledgements	Reduces the number of dropped packets	Routing overhead is periodical broadcasting of trust value calculated to all nodes in the network.
3	Pirzada, Asad Amir, AmitavaDatta , and Chris McDonald. & 2004	Trust TORA	Effort-return based on trust model in a decentralized manner to create self organized reliable network.	Trust agent passively monitor and measure the accuracy of data and control packets that are either forwarded or received.	Overhead increases for maintaining Hash cash tokens which are computed using cryptographic hash functions.
4	MohdZamirArif, et al. & 2013	TDSDV	A secure route maintenance mechanism is provided by involving threshold in terms of packets	protects through unwanted packet flooding of the network and increases network performance	Threshold value to be treated as intruder and the path is rediscovered with the new threshold value and discarding the intruder node.
5	Abusalah, Loay, et al. & 2006	TARP	To evaluate shortest path using battery power and software configuration.	Reacts quickly and effectively to the dynamic of the network and also finds the shortest path to the destination.	The major issue is to determine the trust metric based on a given set of attributes.
6	] Asma Adnane, Christophe Bidan , Rafael Timóteo de Sousa Júnior & 2013	Trust OLSR	Semantic properties of OLSRs in terms of trust are analyzed and implicit trust related properties in OLSR are identified to detect malicious nodes.	Allows to verify if the behavior of other nodes in the network Complete with the specification and Ensures efficient routing operation of OLSR validity of the topology	Implicit trust relations and no explicit which helps to identify whether the underlying assumptions for the operation of a protocol are realistic or not