A SURVEY ON TRAS: TRUST BASED ROUTING PROTOCOL FOR AD-HOC AND SENSOR NETWORKS

Sameera Tasneem[1], Mr. Natesh. M[2]
[1]PG Scholar, [2]Associate Professor
Department of CSE, VidyaVardhaka College of Engineering, Mysuru, India

ABSTRACT: Now days the technology is improving day by day. The technology of wired network has been changed to the wireless network. There are many advantages of wireless network over wired network that wireless has better mobility and reliability than wired. One of the main Advantage is we can walk around freely in a network area and accesses internet. In the wireless network, Security is one of the major challenging issues in a mobile ad-hoc network (MANET).Wireless sensor and ad hoc networks are gaining a lot of attention in research due to their importance in enabling mobile wireless nodes to communicate Routing protocol in wireless sensor and ad hoc networks discover a multi-hop route between source and destination nodes. The TRAS: a Trust based routing protocol for Ad hoc and Sensor networks. In the TRAS protocol the trust is an important factor for successful communication. This paper presents a survey on routing protocol and trust in MANETs.

Keywords: mobile ad-hoc network (MANET); wireless sensor network (WSN); routing protocol; security; trust.

I. INTRODUCTION

Wireless Sensor Networks (WSN) consist of Nodes, there can be several hundreds or even thousands. A Mobile Ad Hoc Network is a network having a number of nodes. Mobile Ad-Hoc network (MANET) is infrastructure-less, self-configuring network, comprised of several wireless nodes. In mobile ad hoc network (MANET), nodes cooperate to dynamically establish the network configuration to find the routes and to maintain routes for message exchange. Similarly same strategy is used in wireless sensor networks (WSNs). Which are capable of communicating with each other where each node forward packets for other nodes for this purpose, a routing protocol is needed, routing protocol in mobile ad hoc and sensor networks discover a multi-hop route between the source and destination nodes. Some routes may not be reliable and trustable, so to have a reliable communication trust has to be maintain between the nodes to forward the packets between the source and destination node, and hence the trust is maintain to enhance the security of communication. TRAS is a concept where the routes are responsible for forwarding the packets during communication. Trust and security are achieved by maintaining the trust factor by the nodes in the network. The trust factor is increased and decreased based on the transmission of the packets during the communication. The trust factor is increased on successful transmission of the packets during the communication between the source and destination, whereas the trust factor is decreased if the node fails to transmit or forward the packet to neighboring node.

Trust is extracted from social relationship. When we have some interactions with somebody, although not so much, a general opinion will be formed. However, if somebody is completely new for us and we have to do business with him, what should we do? Perhaps, there are some friends of ours knowing him. Then we collect their opinions. From the information gathered, we get our own choice. It is the same in MANETs. The trust in MANETs can be classified into two -First-hand trust and recommendation [1]. The routing protocol designed for ad hoc networks such as Dynamic Source Routing Protocol (DSR) and Ad hoc on Demand Distance vector (AODV) protocol.

II. BACKGROUND AND RELATED WORK

A lot of work has been done to offer better and more secure routing protocols, for ad hoc and sensor networks. Several Factors are involved in this routing process. The issues of trust and security are very important for many communications Environments and thus it is important to find efficient protocols that can address them. The authors in [2] discuss a trust model for ad hoc networks, and discuss how trust levels can be obtained and used. This model can discover a potentially trustable route for communication and data transmission. Initially, each node in the system is authenticated by an authentication mechanism and is assigned a trust value according to the identity. The routing protocol can then choose the best route according to the current trust levels of the nodes in the ad hoc network. In [3] the authors argue that TCP is not suitable for ad hoc networks and propose a new transport layer routing protocol ATP (ad-hoc transport protocol). This enforces our approach to providing routing at a higher level and allowing the applications to take control of the process. Furthermore, the utilization of middleware to provide this type of functionality is another viable approach. Trust report distribution mechanisms are necessary for the nodes to receive indications of potential threats or trustable behaviors in the network. A simple approach to distributing trust reports is for a node to only broadcast trust reports to its immediate neighbors. This means that each node would maintain a trust level table that includes only the next hop for each route. The nodes would then select routes based on solely the trust levels of its neighbors. Once a data message transmission is initiated, each node along the route would evaluate the route against its own trust level table. The author L. Capra in 2004[4] the trust concept is important for communication and network protocol designers when creating trust relationships between participating nodes. Trust is also defined as degree of belief about other entities behavior. Trust is paramount to ensure collaborative optimization of system metrics. The paper in Trust Management Model for Mobile Ad-hoc Network Based On Analytic Hierarchy Process and Fuzzy Theory, the author proposed that Fuzzy based trusted dynamic source routing protocol have been proposed by H. Xia et al in 2011, [5]. This trust model uses the concept of analytic historical theory (AHT) for the computation of trustworthiness of each node and the node future trust is evaluated by Fuzzy theory. The main drawback of this routing protocol is that it requires to exchange recommendation among nodes i.e. routing overhead is very high for FTDSR. In the paper Trust Prediction and Trust-based Source Routing in Mobile Ad-hoc Networks Xia et al in 2012, [6] has proposed a routing protocol named as trusted source routing protocol (TSR). In TSR, trust among nodes is classified into three categories – Node historical trust, node current trust and the route trust. Node historical trust is computed with the help of packet forwarding ratio and the node future trust is predicted with the help of fuzzy prediction theory. TSR improves the throughput and packet forwarding ratio when compared with other DSR routing protocols. From the survey it is analyzed that the performance of Dynamic Source Routing Protocol increases when it uses the security mechanism and it is also analyzed that the performance of DSR is higher when the concept of trust is fortified with it. In the paper CORE (Collaborative Reputation) by Michiardi and Molva’s proposed in 2002[7]. It author says that has a monitoring mechanism Complemented by reputation functionality that differentiates Between direct reputation, indirect reputation, and functional Reputation. The reputation is calculated based on various types of information on each entity's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented. The proposed protocol is developed to make decisions about cooperation or the gradual Isolation of a node. A unique characteristic of this mechanism is that it exchanges only positive reputation information. However, this may limit its reliance on positive reports without the facility to submit negative feedback. In He, Wu, and Khosla’s [8] work, a reputation-based trust management scheme using an incentive mechanism was introduced (secure and objective reputation-based incentive; SORI). This scheme encourages packet forwarding and discourages selfish behaviors’ based on quantified objective measures and reputation propagation by a one-way hash chain based authentication. The performance of this scheme in the presence of malicious nodes, as may be expected in a hostile environment, has not been investigated. The author Zeeshanali Shaikh1, B.B. Gite1 in Design of Trust Aware Routing 2016[9] came out with the idea of trust management, Where TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. The paper has designed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment, with the idea of trust management. In this paper Different Ways to Achieve Trust in MANET Renu Dalal , Manju Khari and Yudhvir Singh, in 2012 [10]. The author has surveyed the existing trust schemes for mobile ad-hoc network to achieve the security and trustworthiness. It is concluded that, Protocol based trust scheme evaluate the trust through indirect communication but System level trust scheme is more feasible as compared to Protocol based. System level trust model uses concept of punishment or reward for nodes and it calculates trust value on the basis of direct communication. Maturity based model is best as compared to Cluster based. In PKI based schemes, self organized scheme is more efficient than Distributed scheme of PKI. Some schemes like individual level trust model CRFSN, PTM etc, threshold cryptography, and cluster & non cluster based certification schemes in MANET are not covered in this paper. In future work, we plan to continue towards with unified trust model scheme.

III. TYPES OF ROUTING PROTOCOL

In this section, we discuss about different types of routing protocol designed for Ad hoc network it includes: Trust based routing protocol (TRAS), Dynamic source routing protocol (DSR), Ad hoc on demand distance vector (AODV), Dynamic trust based routing protocol (DMTR), Trusted AODV (TAODV). In multi hop wireless networks, routing protocol is used to transfer the packets between nodes via intermediate nodes. Basically routing protocol is divided into three phases: route Discovery, Packet forwarding and route maintenance. Routing protocols in MANET are of two types: proactive and reactive protocols. Proactive protocols constantly monitor networks and periodically send messages to all other nodes for up to date view of network. Every node maintain routing table for all other nodes and update regularly when any node moves. Reactive protocols rely on some request-reply messages. It is on-demand protocol i.e. when source requests for connection to destination then these protocols establish routes to destination. The trust model [11] represents how to calculate the Trust of the routing path by using the trust value of individual Nodes. The trust model mainly consists of two phases: trust formation and trust usage for routing decisions. In trust formation phase, each node collects the network statistics like packets forwarded, packets dropped and packets delayed etc., based on which trust of a node is calculated. Though collection of statistics is performed regularly, it is used only when requested routing path contains the node as intermediate node. Once the route from source to destination is requested, all the intermediate nodes calculate their trust values using equation

$$T = \sum_{i=0}^{n} a_i p_i$$

Where *n* is the number of parameters, *ai* is weighting factor of *i*th parameter and *pi* is the trust value of *i*th parameter.

1. An Overview of TRAS Routing Process

The protocol in this paper [12] says that, When an intermediate node y receives the REQ message from a node *x*, it checks if it already processed this message which is uniquely specified by the (*s, d, ID*) tuple. If it already processed this message, it drops it. This prevents looping. Otherwise, it checks if it is the destination indicated in the message. If it is not, it checks its routing table for a path to the destination with the required minimum trust factor. If such path exists, it appends it to the PATH list and unicasts a reply REP(*s, d, ID, x, PATH*) message back to the destination. If a path to the destination does not exist in its routing table, it appends its ID to the *PATH* list in the REQ message and forwards the REQ message to its neighbors that satisfy the trust requirement included in the message (as specified by the application layer of the source). The *PATH* list in the message is an accumulated list of nodes that the REQ message has propagated through. This process continues until the REQ message arrives at the destination node *d*. At that time, *d* unicasts a REP message back to the source *s* along the discovered path saved in the *PATH* list. When the source receives the REP message, it updates its routing table with this information and starts the data transmission process.

In TRAS routing protocol, contains the following Fields:

(s, d, ID, x, tmin, tcum, PATH, NH, MAX_NH, BACKUP_PATH)

1. s: ID of the source node.
2. d: ID of the destination node.
3. ID: Message ID. Which contains (s, d, ID) for every REQ message and is used to prevent Looping.
4. x: The node ID of the host that is forwarding this REQ message.
5. tmin: The minimum value for the trust factor required in the path from s to d.
6. tcum: The cumulative trust factor the path that is being discovered.
7. PATH: Contains the accumulated list of hosts that the REQ message has passed through.
8. NH: Contains the next hop information.
9. MAX_NH: Maximum number of nodes in the NH list.
10. BACKUP_PATHS: This is the maximum number of backup paths that can be included in the routing table of the source node.

If the BACKUP_PATHS is equal to 0 then, the destination selects the path with the highest trust factor i.e. PTF=tcum/n, where n is the number of intermediate nodes in the path.

2. An Overview of the DSR-Based Routing Process

The protocol that is presented in paper [12] is based on the Dynamic Source Routing (DSR) protocol. Nodes do not need to keep information about the entire topology and routes are only discovered as the need arises. When a source node *s* wants to send data to another destination node *d* which is not within its transmission range, it will try to discover a multi hop path to it. To do that, node *s* broadcasts a request (REQ) message to all of its neighbors. Each of the neighbors adds its ID to the Accumulating path in the message and in turn forwards it to all of its neighbors. This process continues until the REQ message reaches the destination *d*, which then unicasts a reply (REP) message back to the source. Upon receiving the REP message the source updates its routing table and starts the data transmission process. A simplified example of the route discovery process is shown in Figure 1.

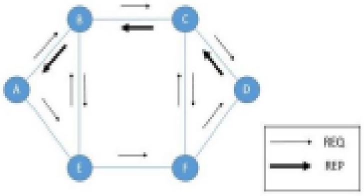

Figure 1: A simplified example of route discovery process.

The DSR protocol operates in two procedures: [13]

Route Discovery

Route Discovery is used whenever a source node, requires a route to a destination node. First, the source node checks the routing table whether if it already contains a route to the destination or not? Source sends the data packet only if the source finds a valid route to the destination. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message.

Route Maintenance

Route Maintenance is used to remove route breaks. When a node confronts a fatal transmission issue at its data link layer, it demolishes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. On receiving a route error message, it removes the hop in error from its route cache.

Advantages:

1. Route is found only when required.
2. All nodes get route cache information.
3. It reduces overhead.

Disadvantages:

1) Route mechanism does not repair the broken links.
2) Higher connection setup delay.
3) Inconsistency may appear in route construction phase.
4) If in case overhead occurs in this routing protocol, path length is directly affected.

3. An Overview of Ad hoc on demand distance vector (AODV)

Ad hoc On-demand Distance Vector (AODV) routing protocol

[14] 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 behaviors 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 communicate with a

destination. Routing maintenance is performed through two ways. One is that a node may positively offer connectivity information by broadcasting hello messages locally so that its neighbors can determine the connectivity by listening for the hello packets. The other way is that a node can maintain local connectivity to its next hops using some link or network layer mechanisms.

4. An Overview of Trusted AODV (TAODV)

A trusted AODV (TAODV) routing protocol was proposed by Li, Lyu, and Liu [15]. Trust is represented by an opinion as used in subjective logic. If a node behaves in a normal manner, other nodes increase their opinions of the node, and vice-versa. The nodes authenticate each other by verifying the certificate. The protocol is unable to detect an internal attack, in which a malicious node may refuse to forward packets or authenticates itself to the source but later on acts as a black hole. In the TAODV, It has also assumed 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 of its one-hop neighbor. In this scheme, TAODV protocol is modified implementing node trust and route trust. Two new control packets are added to TAODV protocol i.e. trust request packet(TREQ) and trust reply packet(TREP) and routing table is modified by adding one new field: route trust. The RREP packet of TAODV is also modified by extending two new fields: neighbor list and route trust.

4.1. Calculation of Node Trust

All the nodes maintain neighbor table to keep information of frequently changing node and node trust value. Node trust value is evaluated using neighbors' collective opinion. The calculated trust value is stored in neighbor table corresponding to a node. Node trust is calculated by observing the behavior of each node. The node trust value (NTV) of a node i is calculated by the following formulae:

NTV=[NNT(1)+NNT(2)+NNT(3)+…….+NNT(n)]/n

Where NNT is the neighbor node trust value about the i node and n is the no of neighbor in the neighbor list.

5. An Overview of Dynamic mutual trust based routing (DMTR)

A trusted routing protocol, called dynamic mutual trust based routing (DMTR) [16], based on the dynamic source routing (DSR) protocol was proposed. DMTR secures the network using the trust network connect (TNC), and improves the path security, which is selected by barrel theory. An exchange of trust tables between nodes require lots of bandwidth, and increase the overhead. Trust management is needed when participating nodes without any previous interactions desire to establish a network with an acceptable level of trust relationships among themselves. Trust management has diverse applicability in many decision making situations, including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes. In DMTR, trust among the nodes is represented by the trust score [trust value], It consist of direct trust score and indirect trust score. Trust updating and routing decisions are based on experienced observed or repeated routing and forwarding behavior of the other nodes, path selection is based on trust score of path. DMTR assume network layer is based on DSR.

IV. CONCLUSION

Wireless network are more popular then wired network. MANET is a Mobile Ad-Hoc Network with no fixed Infrastructure with wireless connection. Security in MANET is critical issue. Trust of discovered multi-hop paths between the source and destination nodes is an important component towards achieving enhanced security in communication. The trust factor is increased when nodes participate successfully during the data transmission process. We have also seen how the trust is calculated. Trust is an important factor in wireless network communication to enhance the security. From the survey we have reviewed different types of routing protocol and showed the overview of different types of routing protocol in MANET based on trust.

REFERENCES

[1] K.Seshadri Ramana, K.Seshadri Ramana , Dr. A.A. Chari Prof. N.Kasiviswanth Trust Based Security Routing in Mobile Adhoc Networks, et al. / (IJCSE) 2010.

[2] Z. Liu, A.W. Joy and R.A. Thompson, A Dynamic Trust Model for Mobile Ad Hoc Networks, Proc. of IEEE International Workshop on Future Trends of Distributed Computing Systems, 2010.

[3] K. Sundaresan, V. Anantharaman, H-Y, Hsieh and R. Sivakumar, A reliable transport protocol for ad hoc networks, IEEE Transactions on Mobile Computing, 4(6)588-603, Nov/Dec 2005.

[4] L. Capra, Toward a Human Trust Model for Mobile Ad-hoc Networks, Proc. 2nd UK-UbiNet Workshop, 5-7 May 2004, Cambridge University, Cambridge, UK.

[5] H.Xia,Z.Jia,L.Ju,Y.Zhu, "Trust management model for mobile ad-hoc network based on analytic hierarchy process and fuzzy theory"Published in IET Wireless Sensor systems2011.

[6] Hui Xia, Zhipingjia, Xin Li, Lei ju "Trust Prediction and Trust-based source routing in mobile ad hoc networks" Computer Communications 2012

[7] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks," 2002.

[8] 8. Q. He, D. Wu and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks," in Wireless Communications and Networking Conference, 2004.

[9] Zeeshanali Shaikh, B.B. Gite, Design of Trust Aware Routing IJARCCE june 2016.

[10] Renu Dalal1, Manju Khari 1 and Yudhvir Singh, Different Ways to Achieve Trust in MANET, April 2012.

[11] Vinesh H. Patel, Mukesh A. Zaveri, and Hemant Kumar Rath , Trust Based Routing in Mobile Ad-Hoc Networks 2015.

[12] Imad Jawhar1, Farhan Mohammed1, Jameela Al Jaroodi2, and Nader Mohamed, TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks, 2016.

[13] Ranjana Sharma Er. Anuradha Panjeta, Shree Siddhivinayak A Secure Trust Based Routing Protocol for MANET ,Aug 2016.

[14] Mousumi Sardar1 and Koushik Majumder, A COMPARATIVE STUDY ON DIFFERENT TRUST BASED ROUTING SCHEMES IN MANET, October 2013.

[15] X. Li, M. R. Lyu and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," 2004.

[16] H. Chuanhe, C. Yong, S. Wenming and Z. Hao, A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks, 2009.