International Journal For Technological Research In Engineering
Volume 4, Issue 9, May-2017 *ISSN (Online): 2347 - 4718*

ETRAS: AN EXTENDED OF 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: Routing protocols in mobile ad hoc and sensor networks gaining a lot of attention in research due to their importance in enabling mobile wireless nodes to communicate without any interruption during the communication. Routing protocol discover usable multi-hop routes between source and destination nodes. However, some of the routes found and used may not be as reliable or trustable as expected. Thus, finding a trusted route is an important component for enhancing the security of communication. This paper presents an Extended of trust-based routing protocol for enhanced security of communication in mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). Enhanced trust and security are achieved by the maintenance of a trust factor by the nodes in the network. This factor is established and the nodes value increases when it participates successfully in data transmissions. The results show an improvement in the trust potential of the discovered path with the proper choice of certain important nodes. This Extended of TRAS is established to avoid unnecessary routing during the route discovery.

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

I. INTRODUCTION

Wireless Sensor Networks (WSN) consist of Nodes, there can be many in number. A MANET is a network which configures itself and nodes are connected wireless. Node in the network or device can often move freely in any direction. In a mobile ad hoc network (MANET), nodes cooperate dynamically to establish a network configuration and find routes for message exchange. In both networks, nodes are responsible for forwarding packets for each other to facilitate multi-hop communication between other nodes that are not in direct transmission range. 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 trust has to be maintained. TRAS [1] 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 [2], 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 similar in MANETs. The trust in MANETs can be classified into two - First-hand trust and recommendation. The routing protocol designed for ad hoc networks such as Dynamic Source Routing Protocol (DSR) and Ad hoc on Demand Distance vector (AODV) protocol. Our protocol is based on the DSR routing protocol, and it is on demand. It is a distributed protocol such as link state based, each node maintain topology and trust information. These characteristics enhance the scalability and performance of the algorithm.

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 [3] discuss a trust model for ad hoc networks, and discuss how trust levels can be obtained and used. This model can discover, potentially trustable route for communication and data transmission. In [4] 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. Trust report distribution mechanisms are necessary for the nodes to receive indications of potential threats or trustable behaviors in the network. 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]. Here the trust model uses the analytic historical theory (AHT) concept 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 exchanging recommendation among nodes and leads to routing overhead which is very high for FTDSR. The author Zeeshanali Shaikh1, B.B. Gite1 in Design of Trust Aware Routing 2016[6] 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 [7]. The author has surveyed the existing trust schemes for mobile ad-hoc network to achieve the security and trustworthiness. Ad hoc On-demand Distance Vector (AODV) routing protocol[8]. This paper describes that AODV is one of the most popular routing protocols for MANETs On-demand is a major characteristic of AODV, where a node only performs routing behaviors when it wants to discover or check route paths towards other nodes. Thus it greatly increases the efficiency of routing processes. A trusted AODV (TAODV) routing protocol was proposed by Li, Lyu, and Liu [9]. 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. TAODV protocol is modified implementing node trust and route trust. Two new control packets are added to TAODV protocol i.e. trust request (TREQ) and trust reply (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. A trusted routing protocol, called dynamic mutual trust based routing (DMTR) [10], 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.

III. THE EXTENDED TRUST BASED ROUTING PROTOCOL (ETRAS)

This section describes the Extended Trust routing protocol (ETRAS). It starts with an overview of the Trust based routing process (TRAS) along with an algorithm. Next, the ETRAS routing protocol data structures, messages, parameters, described along with a detailed example that illustrates the routing process.

A. An Overview of TRAS Routing Process

Intermediate node y [1] 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 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 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, the REQ message is forwarded to its neighbors that satisfy the trust requirement included in the message. *PATH* list in the message is an accumulated list of nodes that the REQ message has propagated through, it continues until the request message reaches 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 Trust factor and starts the data transmission process.

Algorithm 1: The algorithm [1] at an intermediate node in TRAS

When node y receives a REQ message
Let ty be the trust factor of y
Let tmin be the minimum acceptable trust factor of the path
Let ny be the number of 1-hop neighbors of y
Let ntf[z] be the node trust factor of z
Let MAX_NH be the maximum number of 1-hop neighbors that can be included in NH list
NH_temp = ϕ sorts 1-hop neighbour using ntf[z] as key
for(z=1; NH_temp < MAX_NH and z ≤ ny; z = z+1)
do
if(ntf[z] ≥ tmin) then
Add z's ID to the NH_temp list
end if
end for
if NH_temp ≠ ϕ then
tcum = tcum + ty
Let PATH_temp = PATH | y
broadcast REQ(S, D, ID, y, tmin, tcum, PATH_temp, NH_temp)
end if

IV. PROPOSED APPROACH

The Extended Trust Based Routing Protocol (ETRAS), it provides a unique approach of discovering the routes during the route discovery. It includes that instead of broadcasting the data to all the nodes and discovers the route; the source multicasts the request to the nodes that satisfies different parameters in order to avoid unnecessary routing. The ETRAS uses the algorithm of Trust Based Routing Protocol for an intermediate node. It uses a DSR and Ad hoc On-demand Distance Vector (AODV) routing protocol.

In our proposed approach the Extended Trust Based Routing Protocol operates in 5 steps:

A. 1-Hop neighbour identification.
B. Route Request Transmission.
C. Intermediate Node Decision.
D. Route Reply Transmission.
E. Message Transmission.

A. 1-Hop neighbour identification

Each nodes establish a 1-hop neighbour identification, each node identifies 1-hop neighbour by broadcasting the hello message to the neighboring nodes and find the intermediate nodes. Each identified 1-hop neighbors are set with the MAX_TRUST.

B. Route Request Transmission

The DSR protocol operates in two procedures: [11]

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 it discovers a valid route to the destination. If not then, 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. On receiving a route error message, it removes the hop in error from its route cache.
Based on the TRAS and DSR, It requires the following Parameters for the route request transmission. (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, used to avoid Looping.
4. x: Current node ID, forwarding the request (RREQ).
5. tmin: The minimum value for the trust factor required in the path from s to d.
6. tcum: The cumulative trust factor of the path.
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 (to control the flodding and provide better Quality of service (QOS)).
10. BACKUP_PATHS: This is the maximum number of backup paths that can be included in the routing table of the source node, requested by source node (Default 0).
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.

C. Intermediate Node Decision
It uses an intermediate node algorithm. When an intermediate node receives RREQ, it sorts all 1-hop neighbours in descending order using their node trust factor. Current node then adds its own trust factor to the Tcum and further broadcast to its entire 1-hop neighbour.
Algorithm 1: The algorithm at an intermediate node in ETRAS
When node y receives a REQ message
Let ty be the trust factor of y
Let tmin be the minimum acceptable trust factor of the path
Let ny be the number of 1-hop neighbors of y
Let ntf[z] be the node trust factor of z
Let MAX_NH be the maximum number of 1-hop neighbors that can be included in NH list
NH_temp = ϕ
for(z=1; NH_temp < MAX_NH and z ≤ ny; z = z+1)
do
if(ntf[z] ≥ tmin) then
Add z's ID to the NH_temp list
end if
end for
if NH_temp ≠ ϕ then
tcum = tcum + ty
Let PATH_temp = PATH | y
multicast REQ(S, D, ID, y, tmin, tcum, PATH_temp)
end if

D. Route Reply Transmission
The Route Reply Transmission occurs when the source establish a route to the destination, It might receive many route request (RREQ). After receiving the request from the source the destination provides a reply by considering parameters. The destination receives many request, to consider the best path to reply the request the destination node calculate Path Trust Factor (PTF) for every RREQ Path by using the following formula:
PTF=Tcum/n
Where n is the number of intermediate node in the path excluding the source and destination node, Destination node chooses the highest PTF to acknowledge back to the source node with Route Reply (RREP) message. Number of RREP to the source node is decided based on BACKUP PATHS parameters in RREQ message. If BACKUP PATH >0, then the destination sends acknowledgement to the entire requested path.

E. Message Transmission
Message transmission occurs between the source and destination, Message is transmitted using optimal path with highest PTF. Update trust factor based on transmission status for each node participating in data transmission. It sends message in primary path if it gets fails, it decreases the trust factor and on successful transmission of message it increases the trust factor, it tries for 3 times if it gets fails it decreases the trust factor and then chooses the next optimal path for message transmission.

F. Detailed example

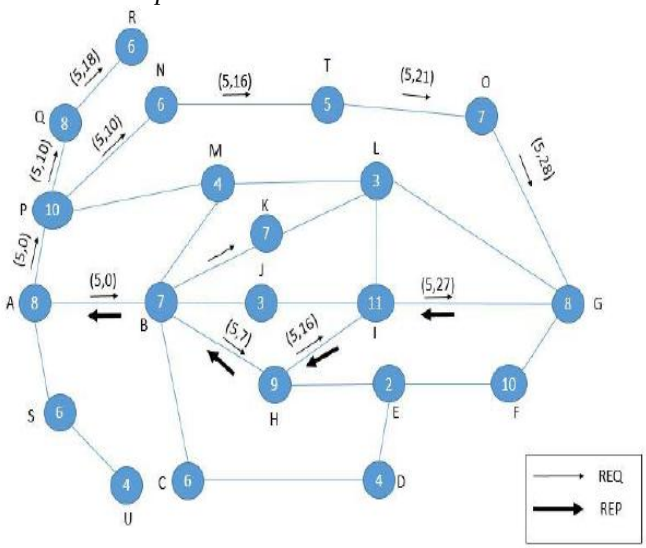

Figure1: Detailed example of ETRAS with route discovery process.

The figure shows a detailed example that shows how the ETRAS process works along with route discovery between the source and destination. Here source is A and destination

is G, source transmit the request to the nodes that satisfies, Tmin=5 MAX_NH=2. Node starts 1-hop neighbour identification for route discovery and sorts its 1-hop neighbors, that satisfies Tmin=5 and future it sort based on MAX_NH=2, here in this example the source A send the request where P, B, S satisfies Tmin=5 but it select only P and B according to MAX_NH=2 i.e. it select two best path with highest factor for route request and drops the other packet. Each node which receives the request will add its trust factor along with trust cumulative factor, as shown in figure i.e. A to B has (5, 0) where (5 is the Tmin and 0 is initial trust cumulative value). Similarly P and B selects its neighbour based on Tmin and sorts it according to MAX_NH and sends the request packet to that respective node and adds its trust factor along with trust cumulative i.e. from B to H has (5, 7) where (5 is the Tmin and 7 is the trust cumulative value) initially it was 0 then it adds its trust factor i.e.0+7=7. The process continues until it reaches the destination G. The destination G selects the route to reply the source. The destination receives multiple requests from the source through the intermediate nodes and it selects only one path to send the reply back to the destination based on PTF i.e. it calculates the PTF value of each request route. The destination G calculates PTF=Tcum/n, where n is the number of intermediate nodes, and PTF is the path Trust factor. In this example the destination get request from the path A-P-N-T-O-G and A-B-H-J-G, destination calculates the PTF of each path and selects the one with the highest trust factor and send the reply in that particular path. According to example destination send reply in G-I-H-B-A. When node A receives the reply, it updates its routing table with the discovered path and updates the trust factor .If the node fails to transmit the data it decreases the trust factor of the node. The destination sends the acknowledgement based on the BACKUP PATHS .If the BACKUP PATH =0 then it sends the acknowledgment to the entire path from where it gets the request. If the BACKUP PATH=1, then it sends the acknowledgement to the only one path which send the reply to the source.

V. CONCLUSION

In this paper Extended of trust based routing protocol for ad-hoc and sensor network, ETRAS was presented with the example. 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 is an important factor in wireless network communication to enhance the security. The ETRAS was proposed to avoid the unnecessary routing during the route discovery. Trust value is increased on each successful transmission of data packet during the communication and decreases the trust factor if it fails to transmit the data packet and sends the acknowledgement on successful transmission based on BACKUP PATHS.

REFERENCES

[1] Imad Jawhar1, Farhan Mohammed1, Jameela Al Jaroodi2, and Nader Mohamed3 TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks 2016 IEEE

[2] 2.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.

[3] 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.

[4] 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.

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

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

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

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

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

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

