International Journal of Electronics and Electrical Engineering
ISSN : 2277-7040 Volume 1 Issue 1
http://www.ijecee.com/ https://sites.google.com/site/ijeceejournal/

TSRD-RL algorithm based Secured Route Discovery for MANET with improved Route Lifetime

S. Priyadarsini

Assistant Professor
Kingston Engineering College,

Vellore, India

priyait46@gmail.com

Abstract. Ad hoc network is collections of wireless mobile devices with limited broadcast range and resources, and no fixed infrastructure. The critical issue for routing in mobile ad hoc network is how to discover a secured path with longest route lifetime and also with minimum node computation. The mobility nature, power constraint of the node and the security attacks of malicious nodes cause frequent path failure. This path failure causes frequent route discovery which affects both the routing protocol performance as well as the node computation overhead. So we propose an efficient Trust based Multipath Route Discovery with improved Route Lifetime algorithm to provide trust based solution for the Security attacks which affects the routing protocol performance. We implement the proposed algorithm in AODV and the performance is evaluated. Our protocol improves the network performance and reduces the computation overhead by avoiding frequent route discovery since we select secured stable multi paths with longest life time. With the help of network simulator we can prove that our proposed protocol performs better than the existing stability-based routing protocols with improved packet delivery ratio.

1 INTRODUCTION

The Mobile Ad hoc Network (MANET) consists of many mobile nodes with wireless communication that can communicate with each other without any physical infrastructure, so it is called as infrastructure less network. The power exhaustion of some nodes and the mobility nature of nodes cause frequent topology changes. So the path between nodes or group of nodes may change continuously.

The node which want to transmit data packets, first needs to discover the route to the destination using route discovery process of different routing protocols. There are two kinds of routing protocols, one is reactive or on-demand routing protocol, and another is proactive or table-driven routing protocol.

Also the routing protocols are needed to be protected from possible internal and external attacks to avoid malicious or compromised nodes to be involved in the route discovery process. The malicious nodes cause in dropping of routing packets without forwarding to destination, sending false route information with expected QOS parameters and discarding the data packets. The security may be provided either using the traditional cryptographic mechanisms; such as digital signature and public key encryption or we can provide trust based security. But both methods have its own pros and cons.

The cryptographic based secure routing requires a key management service to keep track of key and node binding. Traditionally the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. Also every intermediate node needs to encrypt and decrypt the control packets before forwarding it to the next hop neighbour nodes during route discovery phase which involves more computational overhead.

In the trust based secure routing, the trust of every node is calculated by considering the knowledge, experience and recommendation of that particular node's immediate neighbour nodes based on a particular node's communication and behaviour with its neighbour node. Every node maintains the trust value of its one hop neighbour in the trust table. This trust value is a dynamic value. So we need to calculate the trust value periodically, and update the new values with the old value in the trust table.

Due to mobility nature, more computations involved in the route discovery process and the power constraint of the nodes , a host may exhaust its power or move away without giving any notice to its cooperative nodes which causes network topology changes. These changes

may significantly degrade the performance of the routing protocols. So the route needs to be discovered with longest route lifetime with less mobility nature. As the route consists of the number of wireless links, the route lifetime depends on the node life time and individual links lifetime. The route discovery without considering the lifetime of the route leads to frequent route discovery and computation overhead of nodes.

The multipath route discovery concept reduces node's computational overhead by discovering multiple paths for a single route request. If a single path fails, the alternate path can be used without reinitiating a new route discovery process. Thus the security threats and dynamic topology of ad hoc network nodes make the designing of the routing protocol for MANET very difficult. This also results in frequent path breaks and frequent route discovery and node computation overheads. So MANET routing protocols should be designed without any security threats and also the lifetime of the route, trust of the route need to be considered as the routing metrics in order to reduce the number of route discovery processes and also to improve network performance.

The remaining paper is organized as follows, Section I deals with the related works.Section II describes the proposed algorithm and the computational steps involved in route discovery process. Section III presents implementation details and result analysis. Section IV includes conclusion and future works

2 RELATED WORKS

There are basically two types of attacks: Active and Passive. In an active attack, information is inserted to the network and thus the network operation or some nodes may be harmed. In a passive attack, a malicious node either ignores operations supposed to be accomplished by it (examples: silent discard, partial routing information hiding), or listens to the

channel, attempting to retrieve valuable information. We see some of the active attack which affects the route discovery process. [1]

1) **Black hole Attack**: A Black hole is a malicious node that falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a good and valid path to a destination node.
2) **Wormhole attacks:** In a wormhole attack, a malicious node can record packets (or bits) at one location in the network and tunnel them to another location through a private network shared with a colluding malicious node.

3)Colluding misrelay attack: In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater.

Many secure routing protocols has been developed .We will analyse some of the existing secure routing protocols. Ming Yu, et.al, [2] proposed a novel algorithm that detects internal attacks. The route-discovery messages are protected by pair wise secret keys between a source and destination and some intermediate nodes along a route established by using public key cryptographic mechanisms. An integrated protocol called secure routing against collusion (SRAC), in which a node makes a routing decision based on its trust of its neighbouring nodes and the performance provided by them. SAODV is a direct extension of AODV that uses a digital signature to sign routing messages and hash chains to secure hop counts by M. G. Zapata, *et.al* [3] which is expensive for MANETs. Ariadne with Timed Efficient Stream Loss-tolerant Authentication (TESLA) can be considered as an extension of DSR with added security features to prevent attackers from tampering routing information and some other types of attacks such as DOS implemented by Y.C.Hu, *et.al* [4] TESLA is an efficient broadcast authentication scheme, but it requires some extent of time synchronization among the nodes in a MANET. SEAD proposed by Y.C. Hu, *et.al* [5] is based on DSDV and uses one-way hash chains to authenticate hop counts and sequence numbers of routing messages .The security mechanism in SEAD can be TESLA or the shared secret keys between each pair of nodes.

Some of the trust based secure routing includes: Wei Gong, et.al [6] proposed a technique to detect black hole attack in which the trust vector is calculated and normalized to the value between[0,1]. The node with maximum trust is selected to forward the control packets. But fabricating trust recommendations by malicious node is not considered. Menaka Pushpa,et.al [7] proposed Trust based secure routing in AODV routing protocol in which every node maintains two tables namely routing table and neighbour table.RREP control packet is modified to include neighbor list and trust value. Based on the trust estimation of every node's neighbor, the malicious node is detected. But it requires two additional control packets.

To discuss about the lifetime prediction methods, the link stability prediction-based routing (LSPR) algorithm [8] uses relative motion and the distance between two neighbour nodes to evaluate the mean link duration to predict link stability. In LSPR algorithm, the mid nodes forward RREQs after delay which is decided by the mean link duration predicted. Furthermore a forwarding rule which can reduce the number of RREQs forwarded by preceding neighbour nodes is designed. But this protocol is not considering the lifetime of the node. A stability-enhanced routing for mobile ad hoc networks was proposed in [9]. The link expiration time (LET), which is used to assess the stability of link, is calculated accurately in company with the discovery of some available stable routes in reactive manner. Based on the updated LET, the discovery of alternative stable route is determined, which can ensure the continuous transmission of data.

In the lifetime-prediction routing (LPR) algorithm , each node attempts to estimate its battery lifetime based on its residual energy and its past activity.

So we need to consider the merits and demerits of both cryptography based secure routing as well as trust based routing protocols while designing secure routing protocols against security attacks in order to give an efficient solution with less overhead and with improved network performance. Also the lifetime of the route needs to be considered as a metric to avoid frequent path breaks. We can use multipath route discovery in order to reduce overhead involved in frequent route discovery. So we

develop an algorithm which discovers multipath route with longest route lifetime and which having more trust value without any malicious nodes.

3 Proposed Trust based Secured Route Discovery with improved Route Lifetime algorithm (TSRD-RL)

The source needs to discover the route to the destination before transmitting any packets. This proposed protocol considers the lifetime of the route, trust value of the route, as a metric for route discovery and also malicious node detection. If we use cryptographic based secure routing alone to avoid malicious node attacks, after discovered the route the attacker nodes can enter into the network and that nod can attack the network through any compromised nodes. But we cannot detect this in post route discovery phase. In trust based secure routing every node periodically monitors other node's behaviour, so even after discovered route we can prevent malicious nodes using the trust table maintained in every node. But if we send control packet without any encryption technique, the attacker node can alter the entry if it's colluding attack. So our technique combines the merits of both the techniques.

Our algorithm involves following computations:

3.1 Node trust Calculation

The trust values of node A to node B is based on the packet communication between those nodes, Recommendations of other neighbouring node of node B, and the packet loss probability between the nodes. Then the Trust values is normalized between the values [0,1].If the values is greater than the threshold, Then the node is the trusted node to forward the control packets

Evaluating Packet Communication.

We can calculate the packet communication by directly monitoring packets communication of node B. This evaluation measures the ability of

forwarding packets on node B. If node B is node A's neighbour then, number of packets node B had actually forwarded. It should be all out-coming packets from node B expects packets which are from source node B to number of all packets node B responsible for forwarding. It can be computed as all in-coming packets except packet those from source node A to destination B.

Evaluating Packet loss probability.

It is node A's evaluation to node B by directly observing MAC layer link quality between node A and node B on physical layer. This parameter is the probability that the data packet will be successfully transmitted between two nodes A,B. For example, we let each node broadcast a probe packet every second. Suppose that node A has received 6 probe packets from B in the previous 10 seconds, at the same time B found that it had received 8 probe packets from A in the previous 10 seconds. Thus, the loss rate of packets from A to B is 0.4, while the loss rate of packets from B to A is 0.2.Thus, the probability that the data packet will be successfully transmitted from A to B in a single attempt is (1-0.4)*(1-0.2) = 0.48.

Evaluating recommendation.

Recommendation is node A's

evaluation to node B by collecting recommendations about node B from other nodes which should be the neighbour of node B.

Then trust vector is ,

$$T(A \rightarrow B) = [\, {}_{A}PC_{B}, {}_{A}PL_{B}, {}_{A}R_{B} \,] .$$

Every node maintains trust table which maintains trust values of it's neighbour nodes whose trust value is greater than the threshold value. The table have two entries: Node_ID and trust_value.

3.2 Route Lifetime Calculation

The route consists of multiple links and the route is broken if any of the link fails. Thus the route lifetime becomes the minimum lifetime of all links in this route. The Link Life Time (LLT) includes both the node lifetime and the connection lifetime. We introduce Connection Lifetime LC_i to represent the estimated lifetime of the connection C_i, and it only depends on their relative mobility and distance of nodes N_{i-1} and N_i at a given time. The term LN_i denotes the estimated battery Lifetime of Node N_i. Then, the lifetime of the link L_i is expressed as the minimum value of (LC_i, LN_{i-1}, LN_i).

The lifetime of route P is expressed as the minimum value of the lifetime of both nodes and connections involved in route P. Assume that ∑ represents the set of all nodes in route P and that € is the set of all the connections in route P. Thus, the lifetime *Lp* of route P can be expressed as

$$Tp = \min (TN_i, LC_i)$$

$$N_i \in \sum, Ci \in € \qquad (1)$$

From (1), the lifetime *Lp* of route P is estimated from the lifetime of each node and each connection.

Node Lifetime Prediction:

The Lifetime of the node is calculated both based on its residual energy and its past history because the active node that is used for many data-transmissions consumed more energy and have very shorter lifetime. Every *T* seconds node *i* reads the instantaneous residual energy value and the corresponding estimated energy drain rate ev_i is obtained.

Connection Lifetime Prediction:

The route lifetime is the minimum node lifetime or the connection lifetime in a route from (1). Since two nodes of a stable

connection are within the communication range of each other, the connection lifetime may last longer, and they are not a bottleneck from the route to which they belong. Second, it is easier to model the mobility of nodes in a short period during which unstable connections last. The connection time TC_i depends on the relative motion between N_i and N_{i-1}, and the connection is said to be broken when two nodes (N_{i-1} , N_i) are moving out of each other's radio transmission range R.

3.3 Route discovery process

When the source node wants to discover the route to the destination, Every node needs to register with CA and gets valid public-private key pair before it starts communication. It forwards Less overhead RREQ (LRREQ) which is depicted as follows,

$$\mathbf{E_{pu\text{-}d}(S_{id}) \,||\, D_{id} \,||\, E_{pu\text{-}n}(trust\text{-}value,\ lifetime)||hop\text{-}count..)}$$

to neighbour nodes. Then the trust value is calculated and trust table is updated. Node Lifetime is calculated as given in subsection A. Then the node which is having trust value greater than the threshold and also having key append its trust value and forward LRREQ to its next hop nodes. LRREQ is forwarded with accumulated trust value till it reaches the destination.

The destination node collects all LRREQ till timeout. It forwards LRREP to the route which having route trust value greater than the predefined threshold value. Every node calculates LLT and update PLT while Forwarding LRREP. Here only nodes which have valid key can process control packets.

To obtain multipath in single route request from source, The source node wait till timeout and selects all the routes with maximum route lifetime and trust values greater than the predefined trust_threshold and updates routing table with more than one route. Thus we can select multipath for single route request with improved route lifetime and without malicious node involvement.

3.4 Attacks prevention

This provides solution to colluding attack, modification attack and black-hole attack. As the source id is encrypted using the destination node's public key, other attacker node's cannot know the source id and forwards false route reply. Thus it prevents black-hole attack. We are forwarding route request and processing route reply only from trusted nodes by verifying trust table entries maintained in each nodes. So the attacker nodes cannot involve in the route discovery process. We are encrypting RREQ with neighbor's public key. It can be processed only by the node's having valid private key. So attacker node's cannot modify the trust value and also lifetime value. Thus modification attack can be prevented.

PSEUDOCODE OF TSRD-RL ALGORITHM.

The notations used in the algorithm are given as follows:

pu-d: Public key of destination

pu-n: Public key of neighbour

pr-d: Private key of the destination

pr-n: Private key of the neighbour

PLT: Path LifeTime

S_{id} : Source ID

S_{seq}: Source sequence number

D_{seq} : Destination sequence number

//Computation at Source node

Public-private key setup

Forward LRREQ

$E_{pu-d}(S_{id})||\ D_{id}\ ||E_{pu-n}$(trust-value, lifetime)||hop-count..)

Calculate trust value of its neighbor nodes and update its trust table

If trust value of a neighbor > threshold

Forward LRREQ

Else

Do not forward LRREQ

//At every intermediate node

If key is available and not a destination

Decrypt: D_{pr-n} [(E_{pu-n} (trust-value, lifetime)||hop-count.)]

Calculate Node Lifetime

// where En is the residual energy of node i, ev is the energy drain rate

Node Lifetime NLT = E_i /ev_i

Updatetrust-value and lifetime

Forward updated LLREQ

If node is destination and having key

Go to step 8

Else

Discard the packet

//At Destination node

Wait till timeout

Decrypt: $D_{pr\text{-}d}[E_{pu\text{-}d}(S_{id})] \,||\, D_{pr\text{-}n}[E_{pu\text{-}n}(D_{id}, S_{seq}, D_{seq},)] \,||$trust- value , Lifetime)]

If Route trust > threshold

Forward LRREP

Else

Discard LRREQ

Decrypt LRREP using its private key and update lifetime

// At destination

Calculate Link Lifetime

// where N_i and N_{i-1} are two nodes which forms link

$LLT = t\text{-}t_1$

//where t,t1 can be calculated from the eqn.3.6 and 3.7

Decrypt LRREP using its private key

// where i is the set of nodes and connections

Path Lifetime $PLT = \min(NLT_i, LLT_i)$

Select route with PLT > lifetime_threshold AND Route_Trust > trust_threshold

Update routing table

4 IMPLEMENTATION

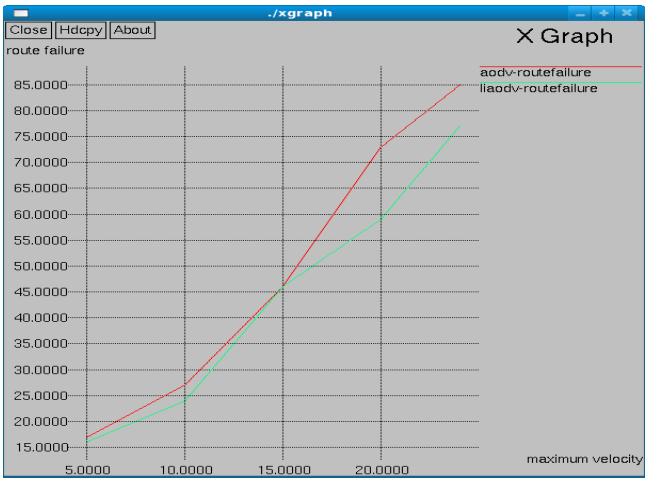
4.1 Simulation Environment

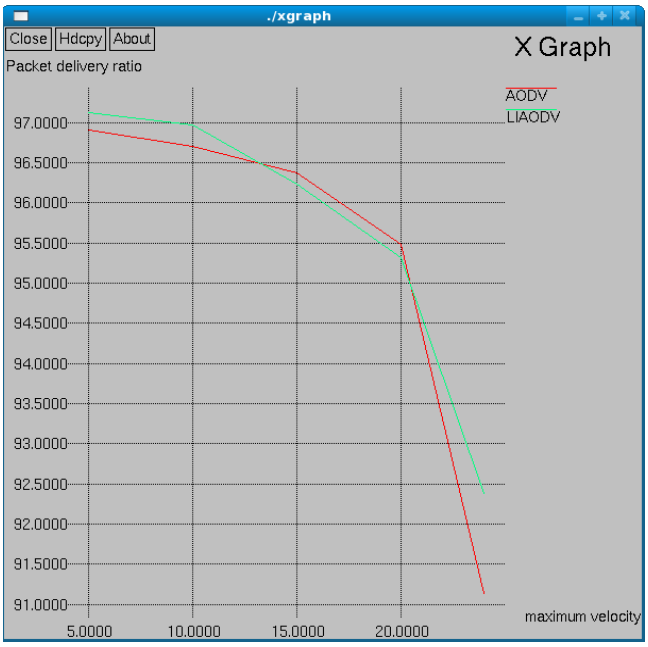
For our simulations, we use a discrete event-driven simulator NS version 2.34. Table 4.1 summarizes the more detailed simulation parameters. The proposed system is simulated with the simulation time of 200ms. The Tcl for proposed system has configured with wireless scenario. The AODV routing protocol is used,

Simulation time	200s
Number of Nodes	50
MAC Type	MAC 802.11
Radio propagation	Two Ray Ground
Energy model	Energy model
Traffic Type	CBR
Routing protocol	AODV
CBR rate	512 bytes
Antenna	Omni Antenna

Table 4.1 Simulation Parameters

A. Result Analysis





5 CONCLUSION

The TMRD-RL algorithm is implemented in NS2.34 using AODV routing protocol. As our proposed route discovery process considers the lifetime of the route, trust values as the metric while selecting the route, the routing failure is minimized. This reduces the number of route discovery process and also the computation overhead of every node involved in route discovery process as it avoids malicious nodes and discovers multipath. To evaluate the performance, proposed protocol is compared with existing AODV with different node velocities. This shows that our proposed protocol reduces routing failure and route overhead. It also improves packet delivery ratio.

REFERENCES

1. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks **" ,** International Journal of Computer Science and Security.

2. X. Wu, H. R. Sadjadpour and J. J. Garcia-Luna-Aceves , "An analytical framework for the Characterization of link dynamics in MANETs," in Proc. IEEE Mil. Commun. Conf., 2006.

3. Ming yu,A secure routing protocol against Byzantine attacks for MANETs in adversarial environment ", IEEE transaction ,vol 58 ,jan 2009.

4. Stephen Dabideen, Bradley R. Smith and J.J. Garcia-Luna-Aceves"An End-to-End Solution for Secure and Survivable Routing in MANETs", IEEE international conference , PP 183-190 ,2009.

5. A.Menaka Pushpa ,"Trust based secure routing in AODV routing protocol" IEEE transaction , 2009.

6. Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, "Trust Based Routing for Misbehaviour Detection in Ad Hoc Networks" journal of networks, vol .5, May 2010.

7. Xi Wu, Jinkuan Wang, Cuirong Wang, "Stability-enhanced Routing for Mobile ad hoc Networks", International Conference on Computer Design and Appliations (ICCDA 2010).

8. X. Wu, H. R. Sadjadpour and J. J. Garcia-Luna-Aceves , "An analytical framework for the Characterization of link dynamics in MANETs," in Proc. IEEE Mil. Commun. Conf., 2006.

9. Xi Wu, Jinkuan Wang, Cuirong Wang, "Stability-enhanced Routing for Mobile ad hoc Networks", International Conference on Computer Design and Appliations (ICCDA 2010).

10. M. Maleki, K. Dantu, and M. Pedram, "Lifetime prediction routing in mobile ad hoc networks," in Proc. IEEE WCNC.