IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 57-62
www.iosrjournals.org

Optimized Link State Routing Protocol Using Detection lgorithm in Manet

Jayanta Das[1], Abhijit Das[2]
[1]*CSE Department, SMTCK, India*
[2]*IT Department, RCCIIT, India*

Abstract : *A mobile ad hoc network consists of mobile networks which create an underlying architecture for communication without the help of traditional fixed-position routers. Nevertheless, the architecture must maintain communication routes although the hosts are mobile and they have limited transmission range. There are different protocols for handling the routing in the mobile environment. This paper will focus on one well known algorithm: Optimized Link State Routing Protocol as well as shared cryptographic technique.*

Optimized Link State Protocol or OLSR is an optimization version of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network, Optimized Link State Protocol or OLSR uses Multipoint Relays (MPR). The idea of MPR or Multipoint Relays is to decrease flooding of broadcasts by decreasing the same broadcast in some regions in the network. Another reduce is to provide the shortest path. The time interval reduction for the control messages transmission can bring more reactivity to the topological changes. [1, 3, 4, 5, 6, 7, 8]

But before this, we need to prevent malicious hosts to enter into a particular zone. These malicious hosts are the victims of several attacks which are discussed later. Attack on a host leads to a malicious host, which interrupt the route in the communication path. Hence a trust based framework is essential to detect and recover from the network layer attacks like black hole attack, wormhole attack and Byzantine attack. Black hole attack interrupts the packets forwarding to the destination. Wormhole attack disrupts the routing and Byzantine attack degrades the routing services. To overcome these attacks the proposed trust based frame work calculates the observed trust value (OTV) and advertised trust value (ATV). The observed trust value refers to the route trust computed by the node itself based on the information in R_ACK and the advertise route trust is advertised by a downstream neighbor. Route selection value is calculated with the observed trust value and advertised trust value. Route selection value (RSV) is used as a metric in selecting one of the multiple paths available to a destination. The path selected by Route Selection Value is the trusted and the shortest path.

Keyword: *MANET, OLSR, Security, Attack, Trust*

I. INTRODUCTION

At first we have to discuss the several threats or attacks with respect of Mobile Ad hoc Network or MANET. [2, 9, 10]

I. Black hole: In this scheme, information is divided into many shares for passing through multiple routes. But in this case, number of shares at source point is more than the number of shares at destination point. If black hole is exist in a particular route, receiver can construct the information from other available shares coming from other routes. In this case, some number of shares is lost.
II. Gray hole: It is same as black hole technique. But unlike black hole technique, information can be constructed at receiving end without losing any number of shares.
III. Worm hole: Inserting one share of malicious node to its partner node will not affect the share arriving at the destination node. But malicious partner cannot get whole information just having a single share.
IV. Jellyfish attack: At the time of sharing information, just delaying one share will not affect the reconstruction state of information at destination node.
V. Spoofing: At the time of sharing information, just missing one share will not affect the reconstruction state of information at destination node.
VI. Sybil attack: In this scheme, Sybil attacker maintains a threshold number of shares for reconstructing information at destination node. But time delay of shares at source node prevents Sybil attacker to collect minimum number of shares for reconstructing information at destination end.

According to shared cryptography technique, information is divided into several numbers of shares which are passed through several communicating nodes and again reconstructed to obtain original information at receiving end. But before this, these nodes should be trusted for preventing from any type of attacks.

II. RELATED WORK

According to Ad-hoc On-demand Distance Vector or AODV Routing protocol [11], shortest path between source and destination nodes is selected. But it is not all times best. According to Secure Ad-hoc On-demand Distance Vector or SAODV routing protocol [12], one-way hash chain and digital signature procedures are implemented. But all these above protocols do not provide any clear information about route dependability. According to Matri et. Al. [13], the watchdog and path rater mechanisms are implemented to collect statistics and to compute trust on routes for Dynamic Source Routing or DSR protocol. According to Liu et al. [14], both cryptography and trust are implemented. But in this case, we have to monitor the neighboring nodes continuously. According to trust based framework [15], a metric known as Route Trust is used to select the trusted path as well as shortest path from the source node. For this purpose, we have to change the routing table entries that mean Route Reply or RREP, Route Request or RREQ and Acknowledgement or ACK packet format. In addition a data structure called Neighbors' Trust Table is maintained by each network node. Our papers proposed that the shared cryptography technique is implemented after determination node trust.

III. METHODOLOGY

For securing Ad-hoc On-demand Distance Vector or AODV [15] Routing protocol, the following changes are made :-

Neighbors' trust table contains neighboring node IDs, their corresponding trust and current number of route sending by node that designated as 'r'. Maximum number of route request is 'R'.

Highest DSN or Destination Sequence Number indicates shortest path between a particular node and destination. It is stored at routing table.

After advertising the Advertised trust Value or ATV by downstream neighbor, Route Selection Value or RSV is computed. This advertisement should go to upstream neighbor by identifying the route to destination as unique Id or Rid. Again Route Selection Value or RSV is implemented as a metric for selecting one out of multiple routes towards destination.

ROUTE_ACKNOWLEDGEMENT or R_ACK is modified version of ROUTE_REPLY_ACKNOWLEDGEMENT or RREP_ACK message under Ad-hoc On-demand Distance Vector or AODV Routing protocol which is used to acknowledge of RREP over an unreliable link. CHOKE packet is used to indicate congestion in the region from a node to its one hop neighbor node. The lifetime under CHOKE packet is set to zero when congestion is cleared earlier than the expected time. Now the node, with specific node ID, broadcast a new CHOKE packet.

IV. COMPUTATION OF ROUTE TRUST

This technique [15] is explained as follows:-

Route trust is computed by every node for each route under routing table for measuring the reliability of a packet for successful arrival at destination. At first, Route Request or RREQ message is sent from source node to destination node and also RREQ set a flag for establishing reverse route from destination node to source node. Each intermediate route under reverse route checks ROUTE_ACKNOWLEDGEMENT packets for computing the route trust which is measured as a ratio of number of packets received at destination node to the number of packets forwarded by source node.

V. COMPUTATION OF NODE TRUST

This technique [15] is explained as follows:-

Every node maintains node trust with respect of it's neighbor nodes. Node trust indicates whether it is possible for a node to send information to its immediate neighbor node or not. Regarding this matter, we take the term Advertised Trust Value or ATV for conveying the trust value by destination node to source node. Another term Observed Trust Value or OTV indicates those values which are stored by source node with respect of all its destinations. Node trust is computed by the difference between Advertised Trust Value or ATV and Observed Trust Value or OTV. A particular node receives an incentive if the Observed Trust Value or OTV is within a tolerable range of Advertised Trust Value or ATV. Otherwise, it is penalized.

VI. CALCULATION OF INCENTIVES AND PENALTIES

This technique [15] is explained as follows:-

Tolerance:

ATV – rt thresh<=OTV<=ATV + rt thresh

Incentives:

When OTV is within the range of ATV.

The incentives will be:

rt = rt + I, where I = rt * (ic/h)

where rt = root trust value, ic = incentive coefficient,
I = incentives
h = distance between source node and destination node in number of hopes

Penalties:

When OTV is either below or above the tolerable range of ATV or node faces congestion.

The penalties will be:

$rt = rt + P$, where $P = rt * (pc/h)$

Where rt = root trust value, pc =penalty coefficient,
P = penalties
h = distance between source node and destination node in number of hopes

VII. ROUTE SELECTION FACTOR

The route selection factor is dependent on node trust on the immediate downstream neighbor M that recommended the route, and on the route trust node M has on the specified route. The route selection criterion is inversely proportional to the number of hops in the route. Many methods can be devised for selecting a route from the available routes. A source node computes the Route Selection Value (RSV) for all its available routes to the destination and it finally chooses the route which has the highest RSV. If two routes have the identical RSV then the following criteria are used to break the deadlock:

- Highest route trust valued route is selected.
- The route with the highest immediate downstream is selected if the routes have same route trust values
- The shortest route is chosen if the immediate downstream neighbors' node trust have same value. If all the above criteria are same then it will select randomly among those routes with same RSVs.

VIII. COMPUTATION OF ROUTE SELECTION VALUE

RSV = tInd/tAvg* RtInd* hAvg/hInd tInd -Trust on the individual neighbor (Node Trust) tAvg - Average of the trusts of all the neighbors that Forwarded /generated *RouteREP*.

RtInd- Trust the individual neighbor has on the Route RtAvg - Average of all the Route Trusts obtained from individual nodes which forwarded/generated the RouteREP hInd - Number of Hops in the route proposed by the individual node in its RouteREP hAvg - Average of all hInd s' obtained from individual neighbors which forwarded the RouteREP.

The equation is normalized with respect to node trust and number of hops to destination

IX. ASSUMPTIONS BEHIND THE CONCEPT

- A unique non zero identification number identifies each node.
- All nodes under network have information regarding total number of bits at the beginning.
- At beginning, all the nodes should be non-malicious with the help of node trust value computed method.
- Between any pair of nodes, a route should be exist.
- Reverse route also should be exist between any pair of nodes.
- All non-malicious nodes, at the beginning should have information about number of shares or m and the threshold value or l.

X. SECRET SHARE CRYPTOGRAPHY ALGORITHM

This technique [15] is explained as follows:-

According to this algorithm, we divide any binary bit file into any m number of shares, passing each share through individual route and again each share can be reconstructed or combined by ORing l number of shares where l<=m>=2. So it can be easily understood that some bits are missing at the time of passing. Let number of missing shares be (l - 1). So with respect of individual bit or multiple group of bits, for a particular bit position, (l - 1) number of shares should have bit missed and (m - l + 1) number of shares should have bit present. Clearly, for every bit position, $^{m}C(l - 1)$ combinations form the mask of size $^{m}C(l - 1)$. Thus '0' on the mask will eliminate the bit from the secret and '1' in the mask will keep the bit generating one share.

As an example, a possible set of masks for 5 shares with threshold of 3 shares is shown below:-

Mask 1: 0 0 0 0 1 1 0 0 1 1
Mask 2: 0 1 1 0 0 1 1 1 0 1
Mask 3: 1 1 0 1 1 0 1 0 0 1
Mask 4: 1 0 1 0 1 0 1 1 1 0
Mask 5: 1 1 1 1 0 1 0 1 1 0

One can easily check that ORing any three or more shares we get all '1's but with less than three shares some positions still have '0's that means remain missing.

XI. MASK DESIGNING TECHNIQUE

This technique [15] is explained as follows:-

List all row vectors of size m having the combination of (l - 1) number of ‘0’s and (m- l + 1) number of ‘1’s and arrange them in the form of matrix. Now the dimension will be , $^{m}C(l - 1) * m$

Transpose the matrix generated in above step. Now the dimension of transposed matrix will be $m * {}^{m}C(l - 1)$. Each row of this matrix will be individual mask for m different shares. The size of this mask is , $^{m}C(l - 1)$ bits, that means, size of the mask varies between m and l.

Let us consider the previous example where m=5 and l=3.

List all row vectors of size 5 bits with 3 number of ‘1’ bits and 2 numbers of ‘0’ bits.

0	0	1	1	1
0	1	1	0	1
0	1	1	0	1
0	1	1	0	1
1	0	1	1	0
1	1	0	0	1
0	1	1	1	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

Size of the matrix is $^{5}C_{2} * 5$ or $10 * 5$

We transpose the above matrix and determine the size of transposed matrix that means $5 * {}^{5}C_{2}$ or $5 * 10$. The transposed matrix is identical of five shares of mask which are previously given.

XII. TOTAL INFORMATION MANAGEMENT

This technique [15] is explained as follows:-

The sending node generates m unique shares by masking the original binary bits file repeatedly with each individual mask.

Next, source node sends all shares towards destination node through multiple disjoint paths. But no two shares should be sent simultaneously.

Now, at destination any l numbers of received shares (where $l<m$) are logically reconstructed to original information with ORing the any l numbers of shares.

After highlighting, route trusting and node trusting, let us discuss the details of Optimized Link State Routing Protocol.

XIII. ROUTING FOR OLSR NEIGHBOR SENSING

The link in the ad hoc network can be either unidirectional or bidirectional so the host must sense the where about of the neighbors. The Hello messages are broadcasted at a periodic interval for the neighbor sensing. The Hello messages are only broadcasted maximum one hop away for avoiding further forwarding. When the first host receives the Hello message from the second host, it sets the asymmetric status with respect of second host in the routing table. When the first host sends a Hello message to second host including second host’s asymmetric status , the second host set symmetric status with respect of first host in own routing table. At last, when second host send again Hello message including symmetric status for first host’s link, then first host changes the status from asymmetric to symmetric. In the end both hosts knows that their neighbor is active and the corresponding link is directed in both ways [7, 8, 17, 18].

XIV. ROUTING FOR OLSR MULTIPOINT RELAYS

The Multipoint Relays (MPR) has key role behind the OLSR protocol to decrease the information exchange overhead. Instead of pure flooding the OLSR uses Multipoint Relays or MPR to decrease the number of the host which is responsible to broadcast the information throughout the network. The Multipoint Relays or MPR is a host’s one hop neighbor which is responsible to forward its messages. The MPR set of host is kept small for the efficient protocol. In OLSR only the Multipoint Relays or MPRs can forward the data throughout the network [16].

When the host gets a new broadcast message, which is need to be published throughout the network and the Multipoint Relays or MPR Selector set consists of message’s sender interface address, then the host must forward that message.

XV. ROUTING FOR OLSR MULTIPOINT RELAYS SELECTION

In this section the proposed algorithm for the selection of Multipoint Relay set is stated. This algorithm is found from [16]. The algorithm constructs the MPR set which includes shortest number of the one hop symmetric neighbors from which it is possible to arrive all the symmetrical strict two hop neighbors. The host must have the details about one and two hop symmetric neighbors for starting the needed calculation for the MPR set. All exchanged information are broadcasted using Hello messages. The neighbors which have status of willingness different than WILL_NEVER in the Hello message can be chosen to act as Multipoint Relays or MPR. The neighbor must be symmetric in order to become an MPR. WILL_NEVER indicates that neighbors which are not willing to act as Multi Point Relay or MPR.

Proposed algorithm for selecting Multipoint Relay set:

1. All the symmetric one hop neighbors which are willing to act as an MPR are taken.
2. Calculate for every symmetrical neighbor host that are two hops away from the calculating source and does not include the source or its one hop neighbors.
3. The neighbor symmetric host to the MPR set is added. If it is the only neighbor from which is possible to get to the specific two hop neighbor, then delete the selected host neighbors from the two hop neighbor set.
4. If there are still some hosts in the two hop neighbor set, then the reach ability of the each one hop neighbor is calculated, meaning the number of the two hop neighbors that are remained by MPR set. Select the node with highest willing value, if the values are the same then the node with greater number of reach ability is taken. If the reach ability is the same, then the one with greater degree counted in the second step is taken. After selecting the neighbor for MPR set, delete the reachable two hop neighbor from the two hop neighbor set.
5. Repeat previous step until and unless the two hop neighbors set is empty.
6. For the optimization, the hosts in the MPR set in the increasing order basing on the willingness is set. If one host is taken away and all the two hop neighbors, covered by at least one host and the willingness of the host is smaller than WILL_ALWAYS, then the host may be deleted. WILL_ALWAYS indicates those neighbor hosts which are willing to act as Multipoint Relays or MPR.

The finding the optimum Multipoint Relays or MPR set for the two hop neighbor coverage is considered to be an NP problem based on [6, 8, 17, 18].

XVI. ROUTING FOR OLSR TOPOLOGY INFORMATION

For exchanging the topological information and building the topology information base the host that were chosen as Multipoint Relays or MPR need to sent the topology control or TC message. The topology control or TC messages are broadcasted throughout the network and only Multipoint Relays or MPR are allowed to forward topology control or TC messages. The topology control or TC messages are generated and broadcasted at periodic interval in the network [16].

The topology control or TC message is sent by a host for advertising own links (at least the links of its Multipoint Relays or MPR selector set) in the network. The topology control or TC message includes the own set of advertised links and the sequence number of each message. The sequence number is used for avoiding loops of the messages and to indicate the freshness of the message, so if the host gets a message with the smaller sequence number it must discard the previous message without any updates. The host must update the sequence number by +1, when the links are deleted from the TC message and also it should increment the sequence number when the links are added to the message. When the hosts advertised links set becomes empty, it should still send empty topology control or TC messages for a certain amount of time, in order to invalidate previous TC messages. This should stop sending the topology control or TC messages until it has again some information to send [7, 16, 17, 18].

XVII. ROUTING FOR OLSR ROUTING TABLE CALCULATION

The host maintains the routing table, with the following routing table information: destination address, next address, number of hops to the destination and local interface address. Next address indicates the next hop host.

The information is received from the topological set (from the topology control or TC messages) and from the local link information base (from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. The information about broken links or partially known links is not stored in the routing table [5, 16, 17].

The routing table is changed if the changes occur in the following cases: appearance or disappearance of neighbor link, creation or removal of two hops neighbor, appearance or disappearance of topological link or editing of the multiple interface association information.

XVIII. STRENGTH OF OUR ALGORITHM

Unlike the previous algorithms [9, 15], this proposed system has two fold protection techniques. These are:

- At first, we determine the node trust and route trust for validating the node as well as route.
- Secondly, the original information is divided in any number of shares and passed between the trusted nodes as well as through trusted routes also.

Besides this, Optimized Link State Routing Protocol becomes more secured by using trust based framework technique.

XIX. CONCLUSION

In this proposed system, it is not clear whether the shared cryptographic system is functioning or not in following conditions with respect of Zone Routing Protocol:-

- If the number of nodes are excessive
- If the number of associated routes are excessive

In future, we should try to minimize the above complexity of the system also.

REFERENCES

[1] P. Jacquet , A. Laouiti, P. Minet and L. Viennot "Performance Analysis of OLSR Multipoint Relay Flooding in Two Ad Hoc Wireless Network Models." Research Report-4260. INRIA, September 2001. RSRCP journal special issue on Mobility and Internet.

[2] Y.Xiao, X. Shen. And D.Z.Du(Eds). " A survey on attacks and countermeasures in mobile ad hoc networks", Wireless /Mobile Network Security , chapter 12, pp 1-38, (Springer, 2006).

[3] Xiaoyan Hong, Kaixin Xu and Mario Gerla "Scalable Routing Protocols for Mobile Ad Hoc Networks." Computer Science Department, University of California, Los Angeles, August 2002.

[4] Koey Huishan, Chua Huimin and Koh Yeow Nam "Routing Protocols in Ad hoc Wireless Networks." National University of Singapore, Singapore.

[5] Ying Ge, Thomas Kunz and Louise Lamont "Quality of Service Routing in Ad-Hoc Networks Using OLSR." Proceeding of the 36th Hawaii International Conference on System Science (HICSS'03).

[6] P. Jacquet, A. Laouiti, P. Minet and L. Viennot "Performance of multipoint relaying in ad hoc mobile routing protocols." Networking 2002. Pise (Italy) 2002.

[7] T.H. Clausen, G. Hansen, L. Christensen and G. Behrmann "The Optimized Link State Routing Protocol, Evaluation through Experiments and Simulation." IEEE Symposium on "Wireless Personal Mobile Communications". September 2001.

[8] A. Laouiti, A. Qayyum and L. Viennot "Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks." 35th Annual Hawaii International Conference on System Sciences (HICSS'2002).

[9] Abhijit Das, Soumya Sankar Basu, Atal Chaudhuri, " A Novel Security Scheme for Wireless Adhoc Network".

[10] Abhijit Das, Atiqur Rahman, Soumya Sankar Basu, Atal Chaudhuri, "Energy Aware Topology Security Scheme for Mobile Ad Hoc Network" .

[11] C.Perkins, E.Royer and S.Das, " Ad hoc on-demand distance vector routing ", RFC-3651(Jul. 2003) .

[12] M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[13] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Network". In the Proceedings of 6th annual conference on Mobile Computing and Networking 2000, 255-265.

[14] X. Li, M. R. Lyu, J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks". In the Proceedings of IEEE Aerospace Conference (IEEEAC) 2004, 1286-1295 .

[15] R. Sathya *, Dr. P. Latha, "PROVISION OF SECURITY USING DETECTION ALGORITHM IN MANET" .

[16] T. Clausen and P. Jacquet "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group, October 2003.

[17] P. Jacquet, P. Mühlethaler, T Clausen, A. Laouiti, A. Qayyum and L. Viennot "Optimized Link State Protocol for Ad Hoc Networks." IEEE INMIC Pakistan 2001.

[18] A. Laouti, P. Mühlethaler, A. Najid and E. Plakoo "Simulation Results of the OLSR Routing Protocol for Wireless Network." 1st Mediterranean Ad-Hoc Networks workshop (Med-Hoc-Net). Sardegna, Italy 2002.