Secure Routing Backup Protocol for MANET from Selective Forwarding Attack

Harsh Lohiya
M. Tech. IV Sem , Dept. of C.S.E.
Oriental College of Technology
Bhopal (M.P) , India
harsh27lohiya@yahoo.com

Rajnish Choubey
Asst. Prof. , Dept. of C.S.E
Oriental College of Technology
Bhopal (M.P) , India
rajnishchoubey@oriental.ac.in

Roopali Soni
Asst. Prof. , Dept. of C.S.E.
Oriental College of Technology
Bhopal (M.P) , India
roopalisoni@oriental.ac.in

Abstract- **In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, thus opening new fields of applications in the domain of networking. One of the most important of these fields concerns mobile ad hoc networks (MANETs), where the participating nodes do not rely on any existing network infrastructure. Self-policing networks such as wireless ad hoc networks face a number of problems to retain trustworthiness and cooperation of the network. Selective forwarding attack is one of the harmful attacks against wireless networks and can affect the whole network communication. The variety of defense approaches against selective forwarding attack is overwhelming. In order to avoid the selective forwarding attack, we proposed a scheme of secure data transmission which can forward the data safely, and detect the selective forwarding attack. We judge the trust value of each node to select a secure path for message forwarding to detect the malicious nodes which are suspected to launch selective forwarding attack.**

Keywords-MANET; Network security; Ad-hoc network; Attack; Routing protocols

I. INTRODUCTION

Ad-hoc mobile networks are very dynamic, self organizing , self healing distributed networks which support data networking without an infrastructure. There are two kinds of wireless networks viz. Access point and Ad-hoc networks. In access point, wireless network uses an access point or base station, which acts as hub providing connectivity between two different nodes , wired and wireless LAN, a node and wireless LAN, etc., In ad-hoc networks, direct communication between nodes are possible by using wireless network interface cards, without any access points. Because of its infrastructure less feature, ad-hoc wireless networks provide the facility for the user to use the network services while continuously moving. The application scenario for the mobile ad-hoc networks is emerging in recent years. Three main parameters to be concentrated for the communication in mobile networks are secured routing [3], service location issues [4], routing and security [6].

The selective forwarding Attack was first described by Karlof and Wagner [18]. This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them.

There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behaviour causes a DOS attack for that particular node or a group of node. They also behave like a Blackhole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network. Another form of selective forwarding attack is called Neglect and Greed. In this form, the subverted node arbitrarily neglecting to route some messages [1]. It can still participate in lower level protocols and may even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between nodes.

The schemes for defending against selective forwarding attack can be classified according to two types of criteria i.e. nature of scheme and defense of scheme. The nature of scheme can be classified into two classes, distributed and centralized. Defense of scheme can be classified into two classes, detection based and prevention based.

A. Distributed and Centralized

In Distributed based schemes, both node and base stations are responsible for detection and prevention of selective forwarding attack and malicious nodes. On the other hand in centralized based schemes only base station or cluster head are responsible for countering the selective forwarding attack.

B. Detection and Preventions

Detection based schemes detect malicious node or the attack or both. On other hand the prevention based schemes

only by pass or ignores the malicious node and are not capable of detecting the attack and malicious nodes.

Selective forwarding attack is one of the harmful attacks against wireless networks and can affect the whole sensor network communication. The variety of defense approaches against selective forwarding attack is overwhelming. In order to avoid the selective forwarding attack, we proposed a scheme of secure data transmission which can forward the data safely, and detect the selective forwarding attack. We judge the trust value of each node to select a secure path for message forwarding to detect the malicious nodes which are suspected to launch selective forwarding attack. Different from the multi-path routing which only defends the selective forwarding attack, our method may find the malicious nodes.

II. RELATED WORK

To prevent routing misbehavior or selfishness in MANETs, various solutions have been proposed previously which can be roughly classified [6] as:

A. Secure Routing Based Scheme: Aims at securing the establishment and maintenance of routes.

B. Credit Based Scheme: Specifically address forwarding of packets for other nodes.

C. Reputation Based Scheme: Aims at reactively detecting misbehavior and proactively isolating misbehaved nodes to prevent further damage.

S. Marti et al. [3] proposed a reputation-based scheme in which two modules (i.e. watchdog and pathrater) are added on at each node. Watchdog module maintains a buffer of recently sent or forwarded data packets. Buffer is cleared only when watchdog overhears the same packet being forwarded by the next hop node over the medium and if a data packet remains in the buffer too long, the next hop neighbor is suspected to be misbehaving. Based on watchdog's suspicion, Pathrater module maintains a rating for every other node in the network and calculates a path metric by averaging the node ratings in the path and then chooses the best path. Main advantage of this scheme is that it can detect misbehavior at the forwarding level as well as in link level. But it might not detect misbehavior in presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior and partial dropping.

Sonja Buchegger et al. [7] proposed CONFIDANT protocol which is based on selective altruism and Utilitarianism. In CONFIDENT, trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. It consists of four modules: The Monitor, the Reputation System, the Path Manager, and the Trust Manager. Each node monitors the behavior of its next-hop node continuously and if a suspicious activity is detected, information of the suspicion is passed to the Reputation System. The Reputation System changes the rating of the suspected node which depends on how significant and how frequent the activity is and if rating of a node becomes less than certain threshold, control is passed to the Path Manager.

To prevent selfishness in MANET, K. Balakrishnan et al. [8] proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehavior by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets.

Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore can not be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes.

K. Vijaya et al. [9] proposed another acknowledgement based scheme similar to TWOACK scheme, which is also integrated on top of any source routing protocols. This scheme detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The main idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a fraction of the data packets will be acknowledged via a 2ACK packet. This fraction is termed as Rack and by varying the Rack, overhead due to 2ACK packets can be dynamically tuned. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Although routing overhead caused by transmission of acknowledgement packets is minimized but this scheme also suffers to detect the particular misbehaving node.

Srdjan et al. [10] proposed a two-fold approach for detection and isolation of nodes that drops data packets. First approach attempts to detect the misbehavior of nodes and will identify the malicious activity in network. It is done by sending an ACK packet by each intermediate node to its source node for confirming the successful reception of data packets. If the source node does not get ACK packet by intermediate nodes then source node send again its packet for destination after a specific time. If same activity was observed again then source node broadcast a packet to declare the malicious activity in the network. Other approach identifies exactly which intermediate node is doing malicious activity. It is done by monitoring the intermediate nodes of active route by the nodes near to active path which lies in their transmission range and by the nodes which are on the active route. Since monitoring nodes are in promiscuous mode and are in the transmission range of intermediate nodes of active route, they can receive all the packets sent along the active route. Monitoring nodes count the number of packet coming into and going out of the nodes of active route. Each monitoring node maintain a list of sent and dropped packets and when number of dropped packets by a particular node exceeds certain threshold, the monitoring node in that range declares that node as misbehaving node and broadcast this information. Upon receiving broadcast packet all neighboring nodes will cancel their transmission to that particular node and enter it into the list of misbehaving nodes. Main disadvantage of this scheme includes the overhead due to transmissions of acknowledgement packets by every intermediate node to the source and working of all nodes in promiscuous mode.

III. PROPOSED WORK

In order to avoid the selective forwarding attack, we propose a scheme of secure data transmission which can forward the data safely, and detect the selective forwarding attack. We judge the trust value of each node to select a secure path for message forwarding to detect the malicious nodes which are suspected to launch selective forwarding attack. Different from the multi-path routing which only defends the selective forwarding attack; our method may find the malicious nodes.

Our protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of attackers, as long as the group members are reachable through non-adversarial path.

Here an authentication framework is used to eliminate outside adversaries and ensure that only authorized nodes perform certain operations (only tree nodes can perform tree operations and only group nodes can connect to the corresponding multicast tree).

Our protocol mitigates attacks that try to prevent a node from establishing a route to the multicast tree both in route request and route reply.

Our protocol involves following steps

(1) Trust key computing

(2) Secure node authentication

(3) Secure route discovery across the node.

```
Select a node to destination
Check selected node in fresh_route cache
If yes then
    Route is confirmed
Else
    Select another new secured node
End if
```

(4) Backup node setup phase.

(5) Route maintenance across the node.

A. Trust Key Computing

There are lots of protocols have been devised to secure ad hoc mobile wireless protocols using cryptography. These cryptographic protocols work under the presence of a central authority.

A new parameter weight value named TLv can be used to choose the best path which ensures reliability of the path by calculating the trust value of the neighbor nodes and that value can be stored in a priority table. Each time a node sends a RREQ either when it determines that it should be a part of a multicast group, and it is not already a member of that group, or when it has a message to send to the multicast group but does not have a route to that group. An intermediate node after receiving a RREQ packet updates its path in the routing table and add the TLv value of its link and forward it to the next node.

To calculate the trust value a new trust policy has been introduced in link and network layer to calculate a key which can be used to determine the reliability of neighbor node, where the key calculation involves dynamic assignment of weights. The policy resides in route entry trust computing part, operates independently and maintains its individual perspective of trust hierarchy.

An entity gathers information about the data and control packet of its neighboring node and overhears data from the events like whether a packet or control message is dumped and not retransmitted. Based on this, every node will maintain some values in a table for its entire neighboring node.

B. Secure Node Authentication

The authentication framework prevents untrusted nodes to be part of a multicast tree or join a multicast tree. Each node forwards RREQIRREP only when the node from which RREQIRREP is received must be a trust node. Node maintains a neighbor list, when neighbor's calculated trust value is less than the threshold NEIGH UNSECURE, then marked it as not credible and unset enable flag in multicast routing table.

Every source will maintain a table which contains destination host, next hop, interface and the average trust level value for the existing paths available as in Table I. These fields can be updated based on the received RREP messages. An alternative route discovery can be initiated for a significantly low TSTv value for a particular route considering that route non-reliable even if there is no link breakage.

TABLE I. TRUST VALUE TABLE

Destination	**Next Hop**	**Interface**	**TSTv**

C. Secure route discovery across the node

When source node requires the route to destination, source enters the route discovery phase and checks whether adequate “fresh” routes to destinations are already available in the Fresh_route cache. If some “fresh” routes to destination in Fresh_route cache are found, source runs Route confirm process. Otherwise, source runs new secured route discovery process to find a secured new route to the destination node.

Source node broadcasts RD_request to nearby nodes; RD_request includes a sequence number field to distinguish the route discovery process from others , a route content field for node address along the path from S to D and the trust level of the source. After the intermediate node receives RD_request from an upstream node X, it inserts its address into the route content field of the RD_request only if it is in the same trust level of the source by confirming the trust key and then sends this modified RD_request to its neighboring nodes (excluding the upstream node X). The RD_request cache of the intermediate node also records the information, including the sequence number of the RD_request and which neighboring nodes are sent only if the request is not duplicated. Otherwise, the duplicated request is discarded.

If a “fresh” route is available from source to the destination in the Fresh_route cache, the source node S adds the secured fresh route from S to D to the RC_request and then transmits RC_request along this route. When it receives the RC_request, an intermediate node checks its Fresh_route cache to determine whether any other fresh route to D is included. If a “fresh” route is available, the node copies RC_request and puts the route information in the route content field of the RC_request before transmitting the RC_request along this fresh route. If no “fresh” route is available, RC_request is transmitted downstream according to its route content field. Eventually, after D receives the RC_request, RD_reply is sent back to S, and S sends packets through this original route.

D. Backup node setup phase

When RD_request or RC_confirm reaches the destination D, it may gather many secured routes with in a period ‘TC’. The nodes of those routes which D received are compared pair wise from beginning to end to find whether any two paths have a section in common. The final node, excluding destination D, in such a section is the “backup node”. A subset of backup nodes can be gathered from any two secured routes. Then, all the subsets of backup nodes are joined and the BS_ packet that includes each backup node and the partial path from the backup node to the destination node are generated. The destination node then uses BS_packet to separately setup the backup_route cache of those backup nodes, where the BS_packet contains the sequence number of this secured routing process, the address of a back up node under the path from the backup node to the destination. The backup nodes store the partial paths from the backup node to the destination node in their backup_route cache after they receive the BS_packet.

IV. CONCLUSION

Ad-hoc mobile networks are very dynamic, self organizing, self healing distributed networks which support data networking without an infrastructure Security is one of the major issues in MANETs. In order to avoid the selective forwarding attack , Our protocol enhances the routing protocol that solves most of its security flaws, prevents and detects attack.

First, we incorporate a trust key computing model which can be used to choose the best path and ensure reliability of the path by calculating the trust value of the neighbor nodes. Then we perform secure node authentication in which authenticated node can only be participated. We proposed a scheme of secure data transmission which can forward the data safely, and detect the selective forwarding attack. We judge the trust value of each node to select a secure path for message forwarding to detect the malicious nodes which are suspected to launch selective forwarding attack.

REFERENCES

[1] G. Lavanya, C.Kumar and A. Rex Macedo Arokiaraj, "Secured Backup Routing Protocol for Ad hoc Networks" IEEE 2010, p-45-50

[2] Imad Aad, JeanPierre Hubaux, and Edward W. Knightly, Denial of Service Resilience in Ad Hoc Networks, MobiCom' IEEE 2004, p-202-215

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 2000, pp. 255-265.

[4] Yih-Chun Hu, Adrian Perrig, David B. Johnson , Rushing Attacks and Defense in Wireless Ad Hoc Network, WiSe, ACM, 2003, p 30-40

[5] J. Anguera, M. Blesa, J. Farré , V. López , J. Petit ,Topology Control Algorithms in WISELIB, SESENA, ACM 2010, p14-19

[6] S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat Proof, Credit- Based System for Mobile Ad-Hoc Networks," in Proc. of IEEE INFOCOM'03, March 2003, pp. 1987-1997.

[7] Sonja Buchegger Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), June 2002, pp. 226-236.

[8] K. Balakrishnan , D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, March 2005, pp. 2137-2142

[9] K.Vijaya "Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks," TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[10] Srdjan C apkun, Jean-Pierre Hubaux, and Levente Buttya´n, Mobility Help security in Ad Hoc Networks, MobiHoc, ACM 2003, p 46-56

[11] S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies , December 2009, pp. 576-578.

[12] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," in 2008International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[13] Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia, SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, International Conference on Computational Intelligence and Security, IEEE 2009, p 421-425

[14] FengHe, Kuan Hao, Hao Ma, S-MAODV:A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol, IEEE 2008, p434-438

[15] Elahe Sheklabadi, Mehdi Berenjkoub, ,An Anonymous Secure Routing Protocol for Mobile Ad Hoc Networks, IEEE 2011, p 142-147

[16] Intrusion Detection System in wireless Ad-hoc Networks Based on Mobile Agent Technology, IEEE 2010, p 470- 475

[17] R. S. Mangrulkar, Dr. Mohammad Atique, Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network, IEEE 2010

[18] Chris Karlof , David Wagner, "Secure routing in wireless networks: attacks and countermeasures"