IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 16-19
www.iosrjournals.org

A Review on An Unobservable Secure Routing Protocol With Wormhole Attack Prevention In Manet

Vaishali Patil[1], Priyanka Fulare[1], S.S. Patil[2], Nitesh Ghodichor[2]
[1]ME WCC Student, GHRCETW,Nagpur India
[1]Professor in ME WCC, GHRCETW,Nagpur India
[2]Professor in ME WCC, PCE,Nagpur India
[2]Professor in BE C.Tech, PCE,Nagpur India

ABSTRACT : *The Privacy preserving routing is crucial in Mobile ad-hoc network for this require stronger privacy protection. An unobservable secure routing protocol provides complete unlinkability and content unobservability on Mobile Ad-hoc Network. An Unobservable Secure Routing Protocol also helpful to prevent wormhole attack on privacy protection that is based on group signature & public key encryption with multipath RREQ and their timestamp. This technique detect suspicious node with the network, trying to become isolate all suspicious node or any suspicious route, will not consider for transmission & traffic is transmitted via another shortest path.*
KEYWORDS :*routing protocols, security, privacy, wormhole attack.*

I. INTRODUCTION

Mobile ad-hoc network is a collection of wireless mobile devices such as laptops, handheld digital devices, PDA and wearable computers forming a temporary network without the aid of any infrastructure or centralized administration MANET becoming more and more common due to there easy of deployment. Mobile ad-hoc network is the transmission of information from node to node or there is peer to peer communication for this communication or data transmission routing is the main concept while routing the packet security issues must be consider for secure routing mobile ad-hoc network various routing protocols are available but these routing protocols are unable to provide complete privacy protection some ad-hoc networks required stronger privacy protection like defense area, the information should not be disclose to third party attacker while transmissions. Nodes which are involved in the routing should be authenticated to each other and data should be secured while routing from sender to receiver. The proposed scheme an unobservable secure routing protocol with wormhole attack prevention is able to provide high level privacy protection as well as wormhole attack prevention as packet is transmitted sender to receiver.

In wormhole attack, attacker record the information at origin point and tunnel it to the destination but one hope away and retransmit the information in neighborhoods of destination [1].

II. RELATED WORK

There are some routing protocols [7] which are used in MANET and provide different level of privacy protection.

2.1 AODV

Ad-hoc [9] on-demand distance routing protocol is reactive routing protocol therefore route are determine only when needed in AODV protocol hello message , RREQ ,RREP message Hello messages may be used to detect and monitor links to neighbors. When a source node needs to send data, but does not already have a valid route to the destination, it initiates a route discovery process in order to locate the destination. A RREQ packet is disseminated throughout the entire network via simple flooding. The RREQ packet contains the following main fields: source identifier, destination identifier, source sequence number, destination sequence number (created by the destination to be included along with any route information it sends to requesting nodes), broadcast identifier and time-to- live. The destination sequence number is used by AODV to ensure that routes are loop-free and contain the most recent route information. Each intermediate node that forwards an RREQ packet creates a reverse route back to the source node by imprinting the next hop information in its routing table. Once the RREQ packet reaches the destination or an intermediate node with a valid route, the

destination or intermediate node responds by unicasting a RREP packet to the source node using the reverse route. The validity of a route at the intermediate node is determined by comparing its sequence number with the destination sequence number. Each node that participates in forwarding the RREP packet back to the source creates a forward route to the destination by imprinting the next hop information in the routing table. Nodes along the path from source to destination are not required to have knowledge of which nodes are forming the path other than the next hop nodes to the source and destination.

In AODV the identity of node all are disclose to other node are authenticate to each other so data will be secure but not prevented from wormhole attack .

2.2 DSR

DSR [8] is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR uses source routing; it means that the source node knows the whole route to the destination. A complete list of intermediate stations to the destination kept in the header of each data packet. The DSR protocol is composed of two main mechanisms namely route discovery and route maintenance that work together to allow the discovery and maintenance of source routes in the ad hoc network. In DSR, route discovery and route maintenance each operate entirely "on demand".

In DSR source nodes the entire root for destination so it is easy for attacker to attack on particular route as route establish between sources to destination. Attacker can create the tunnel parallel to the main route which is established.

2.3 USOR

Unobservable secure on-demand routing protocol for MANET it offer complete privacy protection in terms of unlinkability and contents unobservability but does not prevent wormhole attack USOR is based on anonymous trust establishment and unobservable route discovery. In anonymous trust establishment the secure key is establish between node for every communication and under that session key route discovery process is takes place to find the route to destination, so identify of node is kept secure from throughout the network and difficult to identify the routing node in the network so it partially as the attacker unable to attack on node which is involved in routing as node is not identifiable

The unobservable routing scheme USOR aims to offer the following privacy properties.

1) Anonymity: the senders, receivers, and intermediate nodes are not identifiable within the whole network, the
largest anonymity set.

2) Unlinkability: the linkage between any two or more IOIs from the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. Note linkage between any two messages, e.g., whether they are from the same source node, is also protected.

3) Unobservability: any meaningful packet in the routing scheme is indistinguishable from other packets to outside attacker. Not only are the content of the packet but also the packet header like packet type protected from eavesdroppers. And any node involved in route discovery or packet forwarding, including the source node, destination node, and any intermediate node, is not aware of the identity of other involved nodes (also including the source node, the destination node, or any other intermediate nodes).

In USOR, an unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. *Disadvantage* of USOR work along this direction is to study how to defend against wormhole attacks, which cannot be prevented with USOR. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

2.4 WORMHOLE ATTACKS

In this attack, an attacker receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network [6]. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long-range wireless link or even through a wired link between the two colluding attackers. Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. If proper mechanisms are not employed to defend the network against wormhole attacks, most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

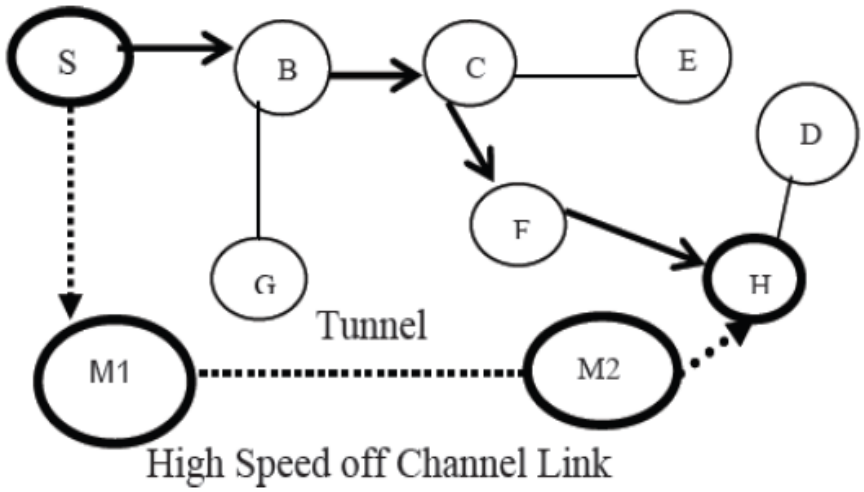

Figure 1: The wormhole attack in MANET [2]

III. PROPOSED SCHEME

The proposed scheme unobservable secure routing protocol with wormhole attack prevention provide the security same as USOR but overcome the disadvantages of USOR by preventing wormhole attack this proposed scheme having three phases anonymous trust establishment, unobservable route discovery and multipath route request with timer calculation[3] .

Anonymous trust establishment: Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors.

Unobservable route discovery: Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node

Multipath RREQ & Timer Calculation: Use to split multipath route so as transmitted data is naturally split into two separate routes an attacker on particular route can not intercept our content [4]. Create many possible routes when sending Route Request (RREQ) from source to destination and to use those routes as reference of each other, in order to find malicious nodes with suspicious behavior within the network. The proposed method works in three steps, which are using routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes. Routes redundancy is started where source sends RREQ using every possible way to destination [5]. All routes that connect source and destination are listed together with the number of hops from every route. Some routes gathered in the same relay point before destination is aggregated, so all nodes that join the network can be listed and the behavior of malicious nodes in can be detected. The RTT and number of hops of all listed routes are compared in order to detect suspicious route.

IV. Conclusion

In USOR, an unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR

not only provides strong privacy protection and also prevent wormhole attack using multipath route request and Timer calculation.

References

[1] Zubair Ahmad Khan"Wormhole Attack: A New detection technique", @2012 IEEE
[2] Pushpraj Niranjan,Prashant Srivastava,Raj Kumar Soni, Ram Pratap "Detection of wormhole attack using Hop-count time delay analysis", IJSRP,vol2,issue4,2012
[3] Zhinguo Wan,Kui Ren, Ming Gu "USOR: An unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" Procedding IEEE Transaction on Wireless Communication,vol11,No.5,May 2012
[4] Soo-Young Shin,Eddy Hartono Halim,"Wormhole Attacks Detection in Manet using route redundancy and Tim-based Hop Calculation", ICTC 2012,IEEE
[5] P.Thamizharasi, D.Vinoth," Unobservable Privacy –Preserving Routing in MANET", IJESE 2013, vol 2, Issue-3, Jan.
[6] Y. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," *Proceedings of IEEE INFOCOM 2003*, vol. 3, pp. 1976-1986, April 2003.
[7] N. Karthikeyan, B. Bharathi, S. Karthik, " Performance Analysis of the Impact of Broadcast Mechanisms in AODV, DSR and DSDV", Proceedings of the 2013 International Conference on PRIME **2013 IEEE**
[8] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless net works," Mobile Computing, pp. 153–181, 1996
[9] C. Perkins, "Ad hoc on demand distance vector (AODV) routing," RFC, pp. 3561, 2003.