EFFECTIVE ANONYMOUS IMPERCEPTIBLE SECURE RE-ACTIVE ROUTING (ISRR) PROTOCOL FOR MANET

Arun Kumar S[#1], A. Mary Mekala[#2]

[#]School Of Information Technology and Engineering
VIT University, Vellore
Tamilnadu – 632014, India
[1]aarunkumar889@gmail.com
[2] amarymekala@vit.ac.in

ABSTRACT

In wireless networks, to provide the privacy protection is a hard one than wired networks. Many protocols in the network use the encryption and decryption technique to transfer the data in a secure way. In wired network, it doesn't need to consider the mobility of the node. But in wireless network it needs to keep the mobility information in the protected way. To give a privacy protection in the network, ISRR protocol tells about the unobservable data transmission. This protocol supports three features: Anonymity, Unlinkability, Unobservability. This paper proposes ISRR protocol, which uses the effective key establishment with neighbor node and also achieves stronger privacy safety over network interactions. This paper focuses on avoiding the type of denial of service attack during packet routing in simulation.

Keywords : AODV, ISRR , DoS, Security, Privacy Protection.

1. INTRODUCTION

MANET which is known as Mobile Ad-hoc Networks is the collection of many mobile users which share more bandwidth with the wireless links. The mobile node helps each other to forward data from a node to node. Selected types of protocols are used for self organizing and routing packets. This protocol exposes the network layer address, neighbors and end points of communication [4]. Some modes of operation will be further mandating that the nodes should tell their physical location freely, and the node should be remained unnamed. The broadcast nature of the wireless networks should be over-come by any method which should help in avoiding eavesdropping. Some of the solutions like encrypting a packet also become useless, because of frequently analyzing the traffic in broadcast networks [8].

MANET environment is always vulnerable for eavesdropping [7]. It is because an intruder can always track the traffic flow in the network and can easily find out the sender and receiver even though the encrypted packet is not cracked. By this the intruder can easily capture a node and destroys it and degrade the network performance. To avoid these types of problems in the MANET, Anonymity should be introduced into mobile networks. Anonymity is the relationship between the sender and receiver cannot be recognized by the other nodes which are present in the network [2].

MANET is the network in which packet delivery in time is guaranteed. So if the routing of the packet becomes misrouted the entire network may get collapsed. In the Ad-hoc networks security is the main factor, which provides privacy to the network [11]. In-order to give privacy based stronger protection; a protocol named ISRR protocol is used. The implementation of this ISRR protocol can be done in two phases. The first phase is the key establishment phase and the second phase is the route discovery phase. In the key establishment phase the RREQ – route request message is sent to the destination. This RREQ reaches the destination and it sends route reply message to the source. When sender receives this route reply message, data transfer between the sender and the receiver begins.

2. RELATED WORK

Zhiguo Wan introduced an USOR routing protocol which is used to provide privacy based strong protection, unlinkability and unobservability of content in Ad-hoc Networks [1]. This protocol is also more resistance to various types of attacks [3]. Ad-hoc On Demand Vector routing protocol commonly known as AODV is the typical routing protocol used in MANETs. For communication between the nodes, one of the nodes in the network starts sending RREQ messages until it finds another node to communicate [10]. When the RREQ

reaches the destination node, the destination node sends an RREP message to the source node. The sender and the receiver nodes communicate through hello messages like RREP messages. These hello messages are shared up to some threshold time limit. When the time reaches the limit the connections between the nodes gets lost.

When the sender node comes to know that the route is not valid it sends an RERR message to all the nodes in the network. This is possible only if the sender node has all the information about its neighbor nodes. In the same way the node which receives the RERR messages initiates again by sending RREQ message to every node to create a new path. By doing all this scheme provides the anonymity and unlinkability but it does not provide the content unobservability – any meaningful packet in the routing scheme is indistinguishable from other packets to an outside attacker. Not only the packets but also the packet header such as packet type is protected from eavesdroppers. In existing system, USOR protocol can prevent the collusion attack and Sybil attack but DoS attack is a challenging task to prevent [1]. So in the MANET, more vulnerable attack named DoS attack called Denial of Service attack, in which the intruder can flood more number of packets and causes traffic to make the network collapse [11]. To mainly avoid this DoS attack the ISRR protocol is used.

3. METHODOLOGY

In this paper a routing protocol is proposed called ISRR. It conserves confidentiality and accomplishes unobservability by setting a group signature using anonymous key signature. The group signature signing key is acquired by each and every node and an ID-based private key from the management scheme of a key or an offline server key [5]. Here there are two phases in routing protocol while execution. In the First phase, by using an anonymous key establishment, secret session keys are built. After that the process of route discovery to the target is performed. The effects of the existing routing schemes have been shown in this paper. The first routing protocol that has been unobservable for wireless mobile Ad-hoc networks named as ISRR, which reaches stronger secrecy in excess of wireless network communications [11]. For an outside attacker, the packet becomes the same. By adjacent with the packets, the packet header like packet type is protected. The node identity concerned in forwarding the packets is not identified to the remaining nodes such as the initial node, target node and any in-between node. On ns2 the comparison is done with the typical performance of AODV and ISRR.

Architecture Diagram

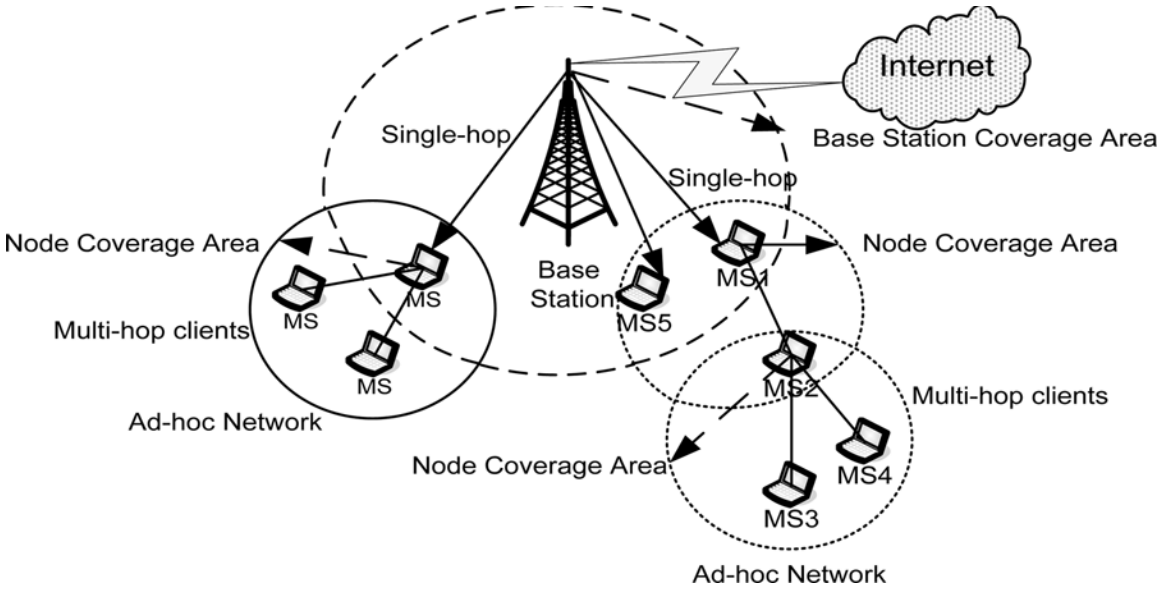


Fig 1: Architectural diagram of ISRR protocol

1) Data Transfer Using AODV

If a node needs to connect with another node by establishing a new route, it broadcasts a RREQ to the whole network until the destination is reached or another node is found. Then a RREP is sent back to the source. Now the route is discovered [9]. Nodes that are part of the new routes shares connectivity information by broadcasting local Hello messages (called RREP messages) to its neighbor nodes. If Hello messages stop arriving from a neighbor at some threshold time, the connection is assumed to be lost. When a node detects that a route to a neighbor node is disconnected it removes the route entry information and sends a RERR message to the rest of the nodes that are active. For this process source node maintains the active neighbors lists. This process is repeated at the nodes that receive RERR messages. A source that receives an RERR can again

initiates a RREQ message to find a new route. This routing process won't consider the energy of the node but only considers the hop-count along the path [6].

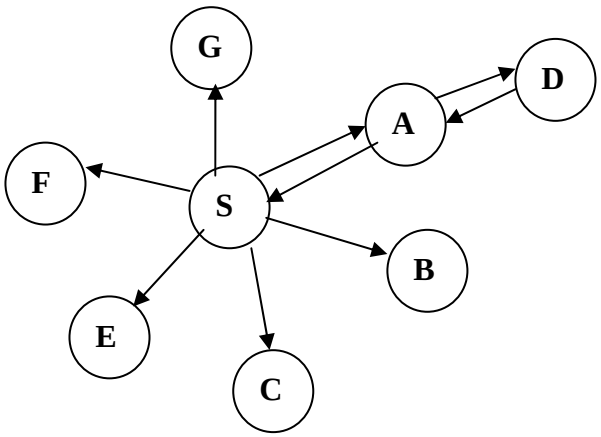


Fig 2 : Data Transfer Using AODV

2) Anonymous Key Establishment

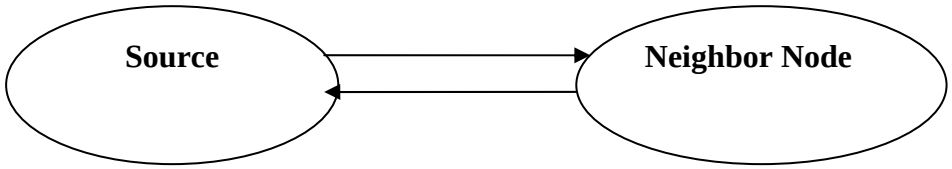


Fig 3 : Anonymous Key Establishment

In this phase, every node in the network communicates with all its direct neighbors within its range for anonymous establishment of keys. For example, if there is a node S with a signing key and a private ID-based key in the network, it is surrounded by a number of neighbors within its radio range [5]. Source node creates the random number and concatenate with the group generator, then it computes the signature and it will send to the neighbor node [9]. Neighbor node checks the signatures of all nodes and creates the session keys.

3) Privacy route Discovery

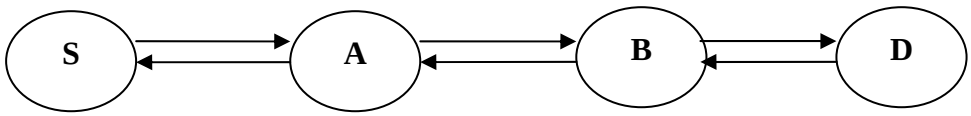


Fig 4 : Privacy Route Discovery

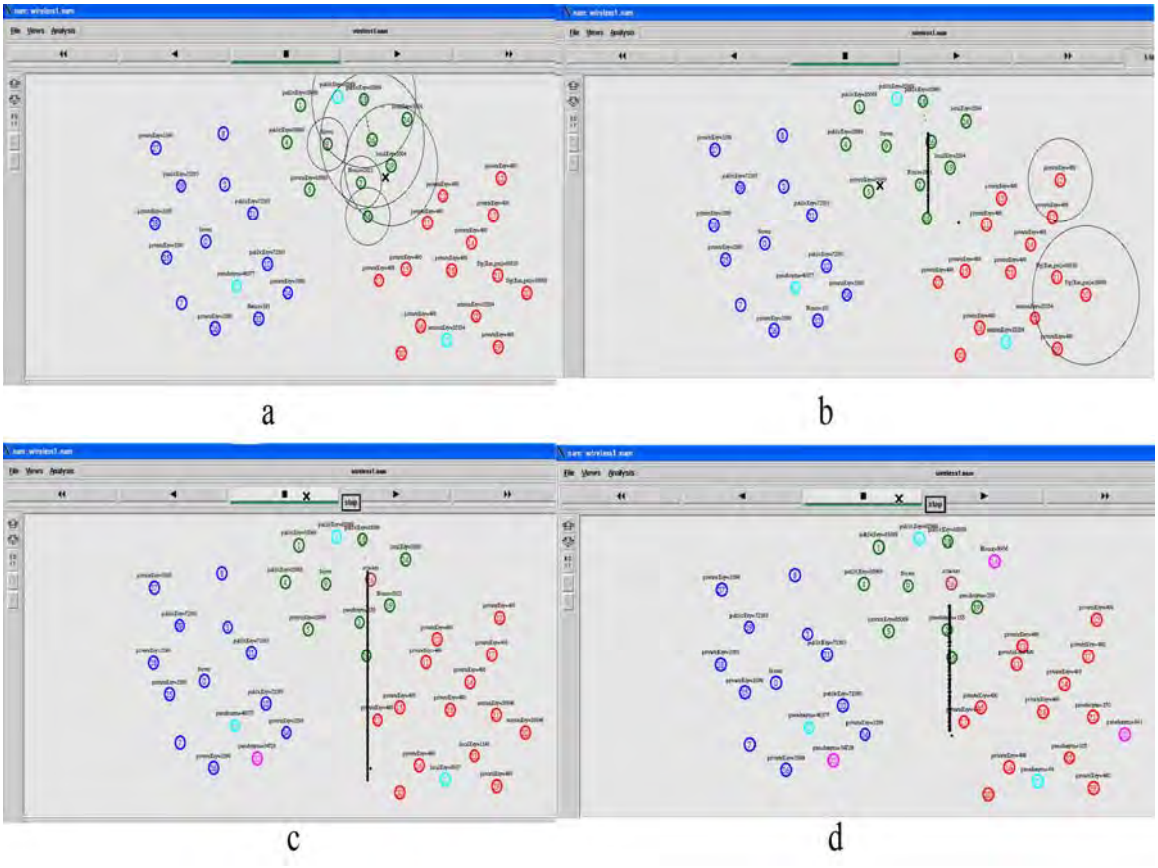
This phase is a Privacy-Based route discovery process which depends on the keys established in last phase [1]. It is similar to the normal route recognizing process, which also includes RREQ and RREP messages that passes through the whole network, while the RREP messages are sent back to the source node only. Each node maintains a table for the RREQ messages and it will send to the nearby nodes by checking the session key and if it matches it will decrypt the route request [2]. If it is not the destination it will send to another neighbor node. This process repeats until it reaches the destination. After reaching Destination the RREP message will decrypts that message and then it will be ready for data transmission using data packets [1].

4) Unobservable data transmission

Source node S can start unobservable data communication under the protection of keys and pseudonyms only after the source node S effectively finds a path to the destination node D [10]. If the source node finds the path, it transfers the data through the neighbor node and also check the pseudonyms of the nodes with received node. It will reach the destination node. Now the source node will identify the path for the destination node and it will sends the data packets to the destination node [9].

4. SIMULATION RESULTS AND DISCUSSION

Here the simulation is done in NS2 to evaluate the ISRR performance and 40 nodes are considered in the network. It considers the key establishment and key distribution in the network. The Network setup considers the packet transfer and speed of the node.



In figure 5. a., the keys are broadcasted to the nearby nodes. The node 26 sends the data to node 18.In b, large number of packets are send from node 26 to node 18. So the data packets start dropping from node 26.In c, the node 26 is found as an attacker. In d, the attacker node 26 is removed from the network.

Performance evaluation

ISRR protocol involves three types of routing control packets, namely routing request packet, routing reply packet, and routing error packet. However, to preserve secret routing information, ISRR wants extra control packets. Due to the privacy property of the ISRR the packet delivery ratio in low traffic load is low compare to the packet delivery ratio of AODV. Route disturbance directs to dropping of packets and packet retransmission. To sent out the remaining packets before only a new path has to be build.

5. CONCLUSION AND FUTURE WORK

In this paper, ISRR routing protocol is proposed to support on the ID-based cryptosystem and group signature for mobile ad hoc networks. The main aim of ISRR suggests well-built confidentiality security-completes unlinkability and satisfied unobservablity for wireless mobile ad hoc networks. The analysis of security exhibits that ISRR affords well-built security and additional resistant in opposition to an attack called DOS i.e, finds the DOS attacker and removes that node from the network. This paper implements the protocol on ns2 and check up the concert of ISRR that gives you an idea about ISRR has acceptable concert in terms of packet delivery ratio.

6. REFERENCES

[1] Zhiguo Wan, Kui Ren, and Ming Gu “USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks”. IEEE transactions on wireless communications, vol. 11, no. 5, may 2012

[2] A. Pfitzmann and M. Hansen, “Anonymity, unobservability, and pseudonymity: a Consolidated proposal for terminology,” draft, July 2000.

[3] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, “On flow correlation attacks and Countermeasures in mix networks,” in PET04, LNCS 3424,2004, pp. 207 225.

[4] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Commun. of the ACM, vol. 4, no. 2, Feb. 1981.

[5] S. Capkun, L. Buttyan, and J. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” IEEE Trans. Mobile Computing.,vol. 2, no. 1, pp. 52–64, Jan. Mar. 2003.
[6] J. Kong and X. Hong, “ANODR: anonymous on demand routing with untraceable Routes for mobile ad-hoc networks,” in Proc. ACM MOBIHOC’ 3, pp. 291–302.
[7] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, “Anonymous secure routing in mobile ad-hoc networks,” in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.
[8] S. Seys and B. Preneel, “ARM: anonymous routing protocol for mobile ad hoc networks,” in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.
[9] L. Song, L. Korba, and G. Yee, “Anon DSR: efficient anonymous dynamic source routing for mobile ad-hoc networks,” in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.
[10] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, “ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks,” Ad Hoc Networks, vol. 7, no. 8, pp. 1536– 1550, 2009.
[11] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, “SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks,” in Proc. 2004 IEEE LCN, pp. 618–624.