ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

Achieving Unobservability through Privacy Preserving Routing Protocol for Ad Hoc Networks

G. Ramachandran, Dr. K. Selvakumar
Department of Computer Science & Engineering, Annamalai University, Tamil Nadu, India

Abstract - A reliable privacy protection technique that is adaptable to different mobile ad hoc networks and it is essential for providing better protection and security to sensitive information. Even though different privacy protecting techniques have been successfully applied, they are prone to fail for protecting all content of packets from the attackers. Moreover, existing methods mainly consider anonymity and unlinkability. In this paper, we propose efficient and effective privacy preserving technique that is USOR method using unobservability. This proposed approach mainly focuses on content unobservability, which improves the privacy condition despite wide in various wireless environments. This paper employs an asymmetry public key cryptosystem that can provide better support for privacy protection. To increase the effectiveness and robustness of the proposed approach, we process an unobservability routing protocol USOR based on group signature and ID based cryptosystem.

***Index Terms*– USOR, ADOV, Adhoc, Unobservability, Unlinkability, Anonymity.**

I. INTRODUCTION

With the progress of information society today, security methods have become more and more important. Among them, privacy protection technique plays an important role in a wide range of network applications. One of the simplest and commonly method which is used in privacy methods is to define password and security code for particular file. Only authorized person can access the content of the file. But in the existing method, the hacker can easily identify password using substitution and transposition technique. Others approaches are ANODR, it's a strong privacy routing method for route discovery and uses a time public/private key pairs. These aforementioned solutions that use single features, although, successfully applied to security protection method but they still suffer from the following. a) Anonymity - provide only anonymity and unlinkability, while unobservability is never considered or implemented by now. b) Unprotected: in current proposals the information like packet types, trapdoor information, public keys are simply unprotected. c) Public key cryptosystem: that they rely heavily on public key cryptosystem and this is a very high computation overhead. In this paper, we propose a novel approach of USOR privacy technique for giving strong protection of content and also consider the comparison between the ADOV and USOR. Content unobservability refers that no useful information can be extracted from content of message. Traffic pattern unobservability refers that no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. First of all, consider a key establishment process to construct secret session keys. Therefore proposed method achieves content unobservavility by employing anonymous key establishment. Secondly, find a route to destination by extending unobservability route discovery process. Finally, analyzing of existing anonymous routing schemes and also demonstrates their vulnerabilities. This paper achieves strong protection over network communications by proposing USOR, Unobservable routing protocol for ad hoc network. In proposed system, largest anonymity is set, so the sender, receiver and the intermediate nodes are not identifiable. Moreover the effort of unlinkability, the linkages between any two or more IOIs, the sender, the receiver, the intermediate nodes and the message is protected from the attackers. The same source also protected from linkage between any two messages. In this approach the outside hacker cannot distinguishable any meaningful packet in the routing scheme. USOR is efficient as it uses a novel combination of group signature and ID based encryption for route discovery. This paper implements USOR on ns2, and evaluates its performance by comparing with AODV. The simulation results show that USOR has satisfactory performance compared to AODV. Route discovery not only identify the source and destination and also aware of all nodes which is involved in the data transmission process.

II. RELATED WORK

Privacy protection is the process of protecting the most important contents and the secret information from the attackers. The related works for this method are discussed below. Anonymity [1] is the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is The set of all possible subjects. With respect to addressees, the anonymity set consists of the Subjects who might be addressed. Both sender and recipient anonymity set anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time. Using anonymity only cannot give privacy preserved data transmission. A mix is a relay device for anonymous communication [2]. However such an approach of single mix archives a certain level of communication anonymity. So this method can easily extend and optimized for more complicated causes. The number of virtual output links of a mix can be very large since they assume a peer to peer mix network. They only

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

maintain virtual queues and the overhead is limited. The main objective of this approach is to analyze the effectiveness of mixes against a special class of timing-based attacks. It is not suitable for the large network. SDAR - secure distributed anonymous routing [3] for wireless mobile ad hoc networks. SDAR introduce the notion of trust management system and it motivates the participating nodes not only to help each other relaying data traffic, but also identify the malicious and avoid using them during the route establishment. RUMAR RIDING: Anonymzing unstructured peer to peer systems [4]. It avoids the complex text understanding technique to distinguish meaningful message. To determine whether a pair of cipher and key rumor hit, it employs a cyclic redundancy check function to attach a CRC value to message. ARM: - Anonymous routing protocol for mobile ad hoc networks [5] scheme proposes the padding scheme for RREQ messages. The source randomly selects a padding length according to the probability distribution in node b that sessions a RREQ message from node a. ALARM: - Anonymous location aided routing in suspicious Manets [6]. Group signature can be viewed as traditional public key signatures with additional privacy features. Any member of a potentially large and dynamic group can sign a message there by only producing length public key that can verify the group signature.

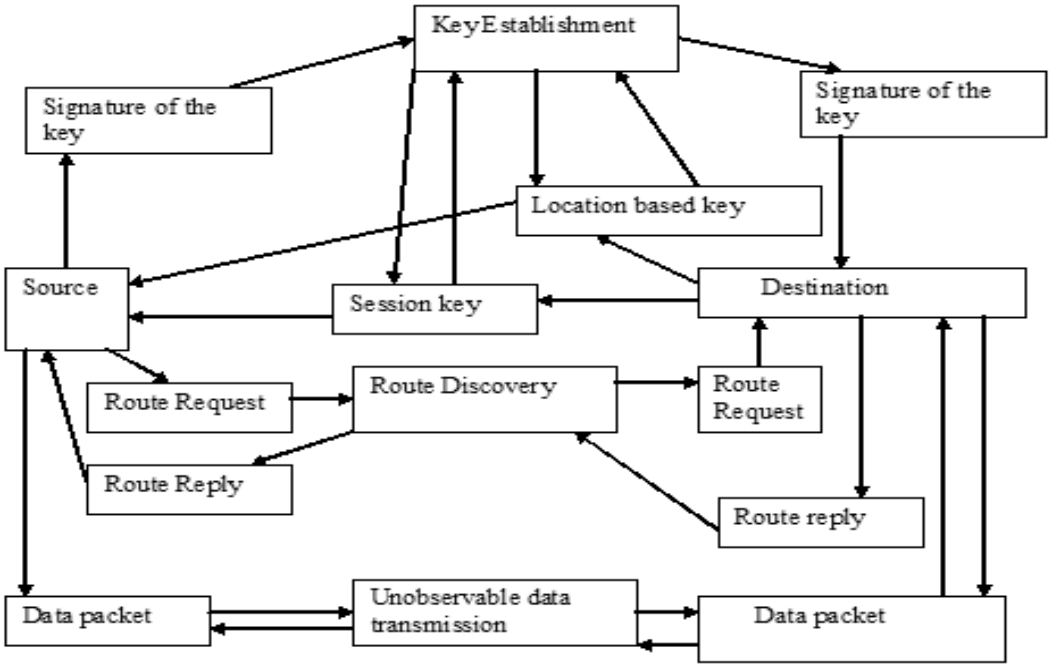

Fig.1. Overview of USOR

III. SYSTEM IMPLEMENTATION

Fig.1 shows the proposed overview of USOR. The complete process involved in transmission of packets from source to destination is explained in a block diagram. First employ a network simulator, which is an even driven simulation tool that has proved in studying the dynamic nature of communication network. Secondly, proposes a privacy preserving protocol USOR and its performance are calculated by comparing it with AODV.

a) Preprocessing

NS is Object-oriented Tcl script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries [7]. To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. C++ is used to define the internal mechanism of the simulation objects. OTcl is used to set up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and OTcl are linked together using TclCL. NS2 is a free simulation tool which runs on various platforms including UNIX Windows & Mac systems. Since, in this paper, Windows based operating system is used, the following method used to install NS2. There are three steps in defining a simulation scenario in NS2.1) Simulation Design, 2) Configuring and NS2. 1) Simulation Design, 2) Configuring and running Simulation, 3) Post simulation processing.

b) Data transfer Using AODV

AODV is a typical routing protocol for Manets. When a node wants to find a route to another one it broadcasts a RREQ to the entire network till either the destination is reached or another node is found with a fresh enough

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

route to the destination. Then a RREP is sent back to the source and the discovered route is made available and it is shown in Fig. 2. Nodes that are part of an active route may offer connectivity information by broadcasting periodically local Hello messages (special RREP messages) to its neighbors. If Hello messages stop arriving from a neighbor beyond some time threshold, the connection is assumed to be lost. When a node detects that a route to a neighbor node is not valid it removes the routing entry and sends a RERR message to neighbors that are active and uses the route. This is possible by maintaining active neighbors list. This procedure is repeated at nodes that receive RERR messages. A source that receives an RERR can reinitiate a RREQ message. This routing process will not consider about the energy of the node and it only considers the hop-count along the path.

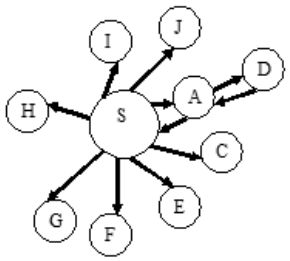

Fig. 2. Data Transmission in AODV

c) Anonymous Key Establishment

Every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment. Suppose there is a node S with having private signing key giving and a private ID-based key KS in the ad hoc network and it is surrounded by a number of neighbors within its power range. Source node generates the Random number catenae with the group generator. Then it computes the signature of that and it will send to the neighbor node. Neighbor node checks the signature and creates the session key. Fig.3 shows the block diagram of session key establishment process between neighboring nodes

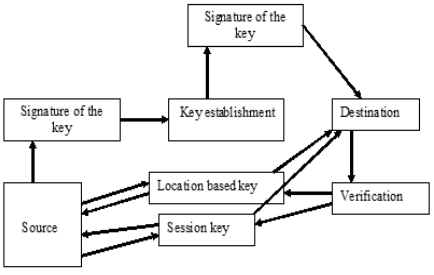

Fig. 3. Session Key Establishment between Neighboring Nodes

d) Privacy preserving routing scheme

The privacy-preserving route discovery process is based on the keys established in previous phase. Similar to normal route discovery process, it also comprises of route request and route reply. The route request messages flood throughout the whole network, while the route reply messages are sent backward to the source node only. Each node maintains the temporary table for the route request and it will send to the intermediate nodes. Intermediate node will check the session key and match the received pseudonyms. If it matches, it will decrypt the route request. If intermediate node is not the destination, it will forward to another neighbor node. This will continue until it reaches the destination which is shown in Fig.4. After it reaches the destination; source node receives the route reply message and decrypts it. Now it will be ready for data transmission of data packets.

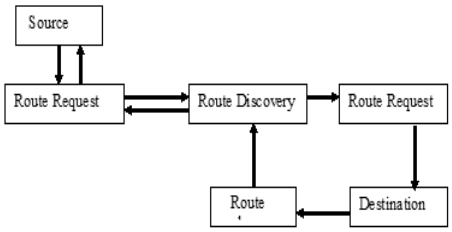

Fig. 4. Discovery of secluded route for data transmission

e) Unobservable data transmission

After the source node successfully finds out a route to the destination node, source node can start protection of pseudonyms and keys which is shown unobservable data transmission under the Protection of pseudonyms and keys which is shown n Fig.5.Source node transfers the data packet and also it checks the pseudonyms of the nodes with received node.

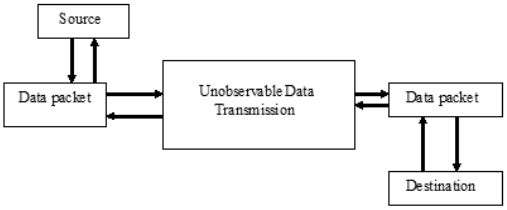

Fig. 5. Data Transmission among Nodes

Finally it will reach the destination node. Source, now knows the destination. Destination will decrypt the message and sends the reply to the source node. The packet delivery ratio decreases as nodal speed increases and traffic load becomes heavier.

f) Performance Evaluation

USOR requires a signature generation and two point multiplications in the first process. In the route discovery process, each node except the source node and destination node needs one ID-based decryption, while the source node and destination node have to do two ID-based encryption/decryption and two point multiplications. AODV requires only three types of routing control packets namely routing request packet, routing reply packet, and routing error packet. However, USOR needs more control packets to maintain anonymous routing information. Due to the privacy property of the USOR, the packet delivery ratio in low traffic load is low

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

compare to the packet delivery ratio of AODV. Route disruption leads to packet drop and retransmission, and a new route has to be constructed before remaining packets can be sent out. Latency also increases due to the operation like encryption and decryption performed by the node. Because of the privacy behavior of the USOR, the packet delivery ratio affected. In AODV, routing process does not done any privacy preserved technique so the packet delivery ratio and latency are better in the AODV than USOR

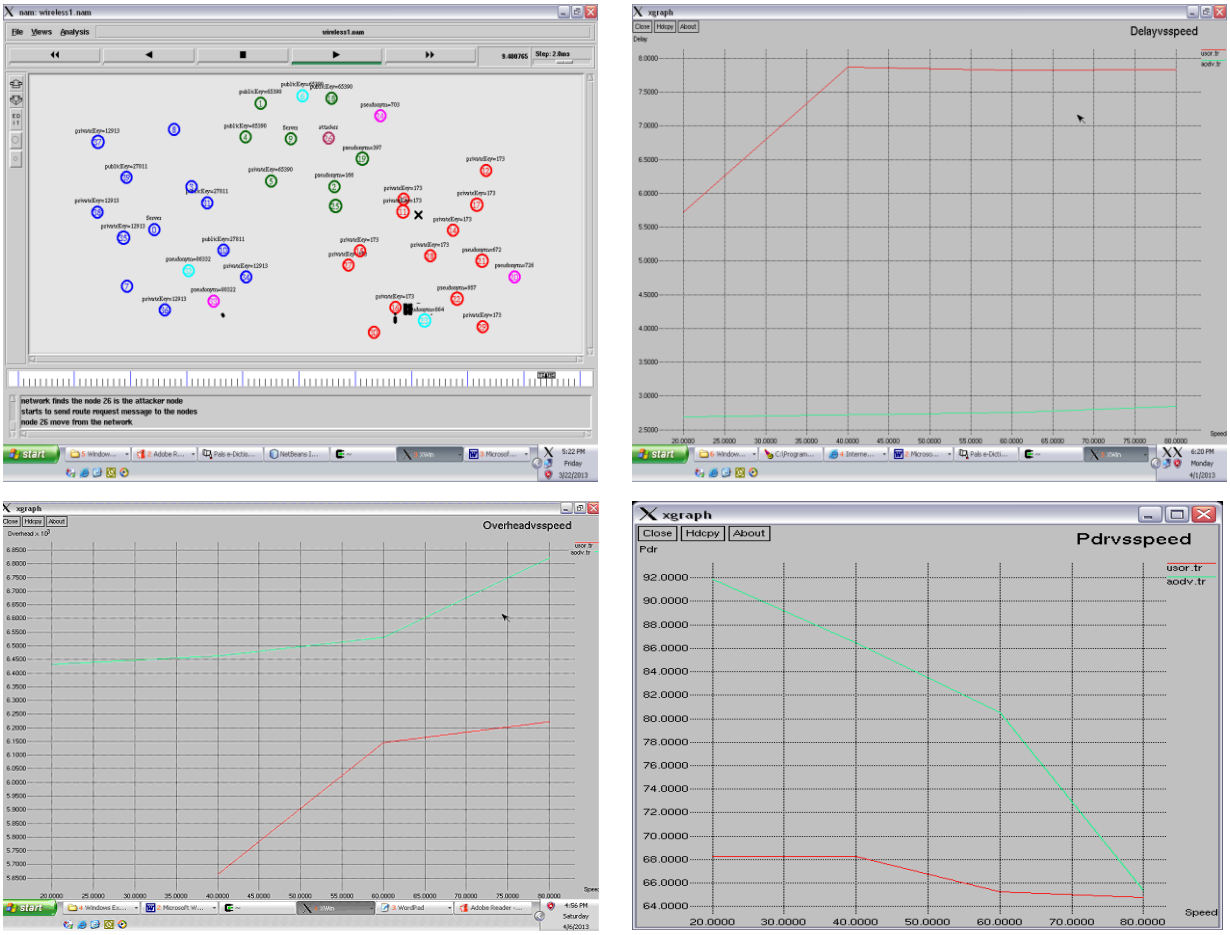

Fig. 6. Comparison of ADOV and USOR

V. RESULT AND ANALYSIS

This paper considers the comparison of packet delivery ratio, delay and overhead of the AODV with the USOR performance. The result is illustrated in Fig.6, in result analysis purpose taken a group of 40 nodes divided into three groups. In AODV, node 0, 9 and 28 are the source node in group 1, 2, 3 respectively. Node 37, 25, 12 are the destination node in group 1, 2, 3 respectively. Then, the route discovery process takes place using RREQ and RREP. After finding the routes to destination, the source node transfer data packets to destination via intermediate nodes. In USOR, nodes are provided with keys by the offline key server. With the help of those keys, each node establishes session keys with their neighboring nodes. Then, node 32 in group 1 sends request to destination node 33. Similar Process takes place in different nodes of group 2 and group 3. When the route is found out, it gets back a reply message. After this process, data packets transfer takes place through that route. USOR based on group signature verification system, so its gives better security protection when compare with ADOV. When the packet drop occurs due to DoS attack, it finds the attacker node and moves it from the network. Here, node 26 in group 2 is an attacker node causing DoS attack. Finding it, node 26 is moved from the network. Fig.6 graph shows the comparison of AODV and USOR in terms of delay, overhead and packet delivery ratio.

V. CONCLUSION

An unobservable routing protocol USOR that offers complete unobervability, unlinkability, anonymity is proposed. The performance of USOR compared with the AODV. Apart from privacy preserving, also demonstrated that USOR is resistant against attacks like DoS. Comparison of USOR and AODV shows the satisfactory performance of USOR in terms of latency and packet delivery ratio. One of the drawbacks of the proposed system is that its success relies on wormhole attacks etc. However, this is the general problem faced by all other researches who work in this domain. Future

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

work can be taken over by considering prevention of wormhole attacks in USOR.

REFERENCES

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

[2] 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.

[3] 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.

[4] Jinsong Han and Yunhao Liu, "Rumor Riding: Anonymzing unstructured peer to peer systems", in parallel distrib. Syst., vol.22, no.3, pp.464-475, 2011.

[5] 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.

[6] Karim El Defrawy and Gene Tsudik School of information," ALARM: Anonymous location aided routing in suspicious MANETs".

[7] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", Springer, 2009.

AUTHOR'S PROFILE

Mr. G. Ramachandran received the B. E degree in Computer Science and Engineering from Annamalai University, Annamalainagar in the year 1997. He received the M.E degree in Computer Science and Engineering from Annamalai University, Annamalainagar in the year 2005. He has been with Annamalai University, since 2000. He is doing his Ph.D. in Computer Science and Engineering at Annamalai University. His research interest includes Computer Networks, Network Security, Mobile Ad hoc Networks and Network Simulator.

Dr. K. Selvakumar received the B.E degree in Electronics and Communication Engineering from Kongu Engineering College in 1989. He received the M.E degree in Communication Systems from Regional Engineering College in the year 1997. He has been with Annamalai University, since 1999. He completed his Ph.D. degree in Computer Science and Engineering at Annamalai University, in the year 2008. He published 30 papers in international conferences and journals. His research interest includes Computer Networks, Cryptography and Network Security, Wireless Networks, Mobile Ad hoc Networks and Network Simulator.