Privacy Preserving USOR Protocol Using Mobile Adhoc Networks

R.Regan, D.Muruganandam, S. Senthil

Abstract— Privacy protection of mobile ad hoc networks is critical issue, compared to wired networks due to the mobility of wireless media. The attacker needs an appropriate transceiver to receive the wireless signal .In wired networks; all the devices are always stable and do not move to any place. Hence in wired network, it's not that much difficult to protect the environments. Collection of nodes that forms a network without the aid of any infrastructure or centralized administration. All the nodes are having limited transmission range. There are two issues plays the critical role for the Mobile ad hoc network i.e Privacy and Routing. Stronger privacy is needed for mobile ad hoc networks. An unobservable secure on demand routing protocol used to provide complete unlinkability and unobservablitiy for all packets. It uses the combination of ID based encryption and Group signature for route discovery. USOR provides security against both inside and outside attackers.

Keywords. – ID, USOR.

I. INTRODUCTION

Ad hoc networks don't have any Pre-established Network infrastructure or topology. An ad-hoc network in terms of wireless is a small LAN network in which each wireless have a ability to directly communicate with the other peer, especially in some wireless connections, in which some of the network nodes are part of the network only for the duration of a session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

In cellular networks the network infrastructure comprises base-stations, Radio network controllers, etc. In ad hoc networks all the communication terminal communicates with its partner node/device to form peer to peer communication. If the required Radio telephone is not a direct neighbor to the initiated call RT then it uses the intermediate RTs are used to form communication link. This is called multi-hop peer to peer communication. This collaboration between the RTs is very important in the ad hoc networks. In ad hoc networks all the communication network protocols should be distributed throughout the communication terminals (i.e. the communication terminals should be independent and highly cooperative).

Mobile Ad-hoc Network (MANET-Self configurable infrastructureless network) is a collection of independent nodes within the network that can communicate using radio waves as medium. The mobile devices that are in range can directly communicate, whereas others make use of intermediate nodes to route their packets.

Manuscript received on April, 2013.

Regan.R , Department of Computer Engineering, University College of Engineering , Pantruti , India.

Muruganandam.D ,Department of Computer Engineering, University College of Engineering , Pantruti, India.

Senthil.S, Department of Computer Engineering, University College of Engineering , BIT Campus , India.

These networks are fully distributed, and can work at any place without the help of any infrastructure. This feature makes these networks highly flexible and robust.

The characteristics of these networks are summarized as follows:

- Nodes can perform either hosts or routers roles.
- No centralized controller and infrastructure. Intrinsic Mutual trust.
- Dynamic network topology. Frequent routing updates.
- Autonomous, no infrastructure needed.
- Can be set up anywhere.
- Energy constraints
- Limited security

In General, the communication terminals have a mobility nature which makes the topology varying and dynamic. The dynamical nature of the network topology increases the challenges of the design of ad hoc networks.Nodes in MANET are mostly energy-constrained. Requires the use of batteries or other form of exhaustible power source. The power consumption of each radio terminal could be divided generally into three parts,

1. Power consumption for data processing inside the RT
2. Power consumption to transmit its own information to the destination
3. Power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network.

Mobile devices usually have limited storage and less computational abilities. They heavily depend on other devices/nodes and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks. MANET also provides the following notions:

A. Anonymity

Nodes in MANET don't reveal its identity within the network and outside of the network. All the nodes are anonymous each other (they don't know about each other). Anonymity has been defined by Pfitzmann and Hansen as ''the state of being not identifiable within a set of subjects, the anonymity set''. The size of this anonymity set is a quantifiable measurement of anonymity. In MANET data communication, anonymity relates to the requirement that the identities of the source, destination and the route of a data message cannot be linked to any node within the network. An additional requirement which relates to the anonymity of data is unlinkability, defined as the notion of a third party (attacker) being unable to distinguish whether any two or more items of interest (in the case of MANETs, data packets) are related. When applied to routing, unlinkability will ensure that data packets from a single flow cannot be linked in order to trace the origin and the destination of this flow.

B. Unlinkability

It gives the security at the time of data transfer, it hides the message. It will not show the what kind of message or data or information transferred between the two nodes.

C. *Unobservability*

In unlinkability, it hides only the data. It will not hide the packet type and packet header information.

II. NETWORK SECURITY

Network security plays a vital role in computer networks, as the vulnerability to the packets transferred over the network increases day to day. Poor design/infrastructure will have high chances of a security risk. Different variables have different impact on security issues and design. Especially environment, origin, range, quality of service and security criticality is variables that affect the security in the network. Security implementations differ on various designs. If the distance between the nodes is more then, the risk of security attacks increases. The nodes are so close to each others that they actually can have a physical contact, some secret information (e.g. secret keys) can be transmitted between the nodes without sending them on air. It increases the level of security, because the wired network is more secure than wireless communication lines.

A. *SECURITY PROBLEMS IN MANETS*

As Ad-hoc networks have no predefined structure of communication and Topology changes dynamically which makes security mechanisms a challenge.

MANET is a self configuring network formed by mobile hosts having wireless communication devices. MANETs consist of mobile nodes interconnected by multihop communications paths and free to move at any speed in any direction and organize themselves randomly.

These nodes are constrained in power , bandwidth, and computational power. Because of MANET's dynamically converging nature it lacks centralized administration and prior organization , security concerns are different than those that exist in conventional networks.

Wireless links make MANETs more vulnerable to attacks. It is easier for hackers to perfoms attacks like eavesdropping, spoofing, Man-in-middle and gain access to confidential information. They can also directly attack the network to delete messages, inject false packets, or impersonate a node(Session Hijacking). This violates the network's chacracteristics such as availability, integrity, authentication, and nonrepudiation. Hackers also use compromised nodes within a network and launch attacks from within a network.

MANETs are much more prone to attack than wired network. This is because of the following reasons :

- Open Medium – Eavesdropping – Hacker steals Information by overlooking into packets using some Protocol analyzers.
- Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- Lack of Centralized Monitoring.
- Lack of Clear Line of Defense - The only use of I line of defense – attack prevention may not sure. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link. In addition to pre-vention, we need II line of defense - detection and response.

MANET security involves authentication, key establishment and distribution, and encryption. Routing protocols in assume preexistence and presharing of public and secret keys for all initial members. These protocols neglect key exchange and authentication, which are very important in MANETs. Recently Zhou and Haas introduced the idea of distributing a CA throughout the network, in a threshold fashion, at the time of network formation. This Distributed Certifying Authority **(**CA) would allow trust relations to be created in the network while also being resilient to some intrusions, malicious insiders, and breaks in connectivity. The resource limitations of devices in ad hoc networks are not addressed. Because public key and threshold cryptography are computationally expensive and require large memory, this method does not meet these resource limitations. Khalili, Katz, and Arbaugh extended this technique to reduce the resources needed by using an ID–based system. Luo et al. developed scalable, distributed authentication services in ad hoc networks. In their approach, multiple nodes collaboratively provide authentication services for any node in the network. In [6], Desmedt gives recent research aspects of threshold cryptography.

An Ad Hoc network in some process and all the measurements and control signals could be transmitted through the network. In order to have secure and reliable control of the process, quality of service requirements need to be met.

Demerits of MANET

- Limited resources: Limited resources -the problem of limited security
- Lack of authorization facilities: Lack of accounting and Authorization.
- Time varying topology: Volatile, changing network topology makes it hard to detect malicious nodes.Security protocols for wired network cannot work for ad-hoc networks.

III. LIST OF AD HOC ROUTING PROTOCOL

An ad-hoc routing protocol is a convention, or standard, that controls and decides how a packet should be routed in the network. Routing Protocols communicate with its neighbor routers and maintain consistency of the routing information at regular intervals In ad-hoc networks the infrastructure is not pre-established so the nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.Thus the network will converge and each node learns information to reach its neighbors (immediate & Multi hop).

Some Ad hoc network routing protocols

A. *Pro-active Routing Protocol*

This type of protocols maintains routing information of destinations and their routes by periodically distributing routing tables throughout the network. It maintains the all the active routes in the network and calculates the shortest path. In this Protocol the overhead is high. Examples of pro-active algorithms are:

- BATMAN - Better Approach to Mobile Ad-hoc Networking.
- OLSR - Optimized Link State Routing Protocol.

B. Reactive (on-demand) Routing Protocol

This type of protocols works on request-response basis, it requests route on demand by flooding the network with Route Request packets. It gets on-demand routes for route discovery and maintenance from DSR. It reduces the overhead by removing the source route in the packet.
Examples of reactive algorithms are:

- ACOR - Admission Control enabled On demand Routing.
- AODV - Ad hoc On-demand Distance Vector.
- DSR - Dynamic Source Routing.

C. Flow-Oriented Routing Protocol

This type of protocols finds a route on demand by following present flows. One option is to unicast consecutively when forwarding data while promoting a new link.
Examples of flow oriented algorithms are:

- IERP - Interzone Routing Protocol

D. Hybrid (both pro-active and reactive) Routing Protocol

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Examples of Hybrid algorithms are:

- ZRP - Zone Routing Protocol.
- First hierarchical protocol combines both proactive and reactive routing protocols.

E. Hierarchical Routing Protocols

In these protocols each node maintains peer's topology information and topology links to them and this information is periodically transferred to the Cluster heads. Each cluster leader broadcast the information to the lower level informing all the nodes about the hierarchical topology of the network
Examples of Hierarchical Routing Algorithms are:

- CBRP - Cluster Based Routing Protocol
  (It groups the nodes in an area together into clusters and for each clusters groups a cluster head is elected. It maintains the complete knowledge on the routing)
- FSRP - Fisheye State Routing Protocol
  (Fisheye has a better view to the nodes when they are nearer to the focal i.e It has more accurate information about the nearby nodes rather than far-away nodes. And it exchanges the topology information only with its neighbors)

IV. UNOBSERVABLE ROUTING SCHEME

A. Anonymous key Establishment

In this phase, every node in the ad hoc network communicates with its direct neighbors within its range for anonymous key establishment. Each node uses anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. There are two parts
i) Node Authentication
ii) Session key Generation

1) Node Authentication

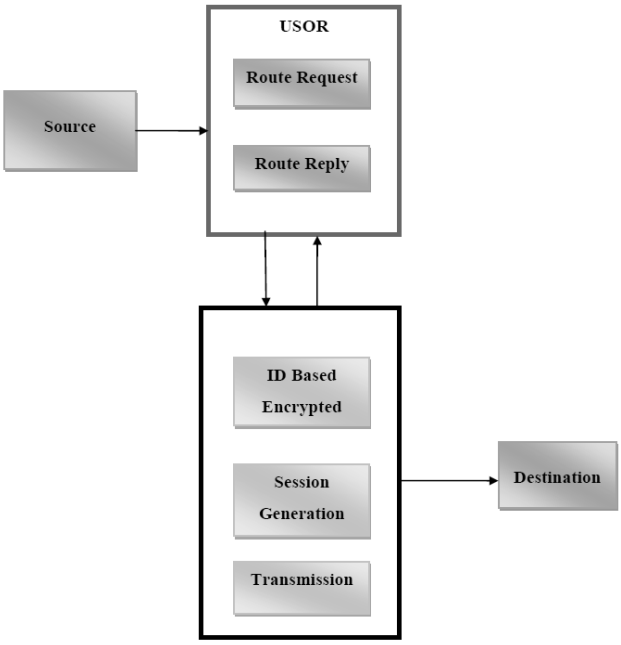
Each node creates its own signing key and generates the signature and send to its neighbor, that neighbor node checks, if the key is valid or not. If the key appears to be valid then it generates the session key and its own signing key and sends to the reply. Group signature and session key both are generated by using the Elliptic curve – Diffie Hellman algorithm.
For example, 'A' wants to communicate with 'B" , then 'A' send its own signing key to 'B'. 'B' checks the key if the key is valid , then it creates the own signing key and Session key replied to 'A'

2) Session Key Generation

Once the keys are valid, 'B' send its signature and generates the Session key and it send the reply to 'A' . 'A' checks the key, if it is valid it generates the Session key. Both the Session keys are matched then it has to do the data transfer. If the session keys are not same, attacker can be identified.

B. Routing

Data transfer is performed by using the route request and route reply. Route request message is flood throughout the whole network (broadcast). Route reply message send to source node only (unicast). Here Nonce (random number) is used to provide the unobservability. Nonce means number used once, once the number is used for communication it will not be reused again. Each route request contains sequence number (unique) and route pseudonym. 'A' chooses a Nonce and calculates a route pseudonym Nym = H(k*|Nonce).



1) Privacy Preserving Route Discovery

This phase is a privacy-preserving route discovery process based on the keys established in the previous phase. Similar to normal route discovery process, the discovery process also comprises of route request and route reply. 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.

a) Route Request

The source node S chooses a random number and uses the identity of destination node D to encrypt trapdoor information that only can be opened with D's private ID-based key. S

selects a sequence number for this route request and another random number as the route pseudonym. It is used as the index to a specific route entry.

Each node also maintains a temporary entry in its routing table. The routing table contains route request sequence number, route pseudonym of next hop, upstream (previous hop) node, and downstream (next hop) node along the route. S maintains the table entry temporally, then S encrypts these items using local broadcast key. At the end, S broadcast unobservable route request to its neighbors. Other intermediate nodes do the same as S does. Finally, the destination node D receives the message from C.D finds out the correct key according to the equation after decrypting the cipher text using records route pseudonyms and the sequence number into his route table. Then D successfully decrypts to find out he is the destination node. D may receive more than one route request messages that originate from the same source and have the same destination D, but it replies to the first arrived message and drops the following ones.

"S" is a source node and intend to send message to destination node "D". The trapdoor information is opened only by using the "D"s private key. Each and every request selects a sequence number (seqno) and another random number Ns as the route pesudonym, which is used as the index to a specific route entry. To achieve unobservability S chooses a nonce $Nonce_s$ and calculates a pseudonym as

$$Nym_s = Nym = H(k^*|Nonce).$$

Each node maintains temporary routing table (seq – no, P-Nym, N-Nym, P-hop, N-hop). Seq-no – Sequence number,P-Nym – Previous Pseudonym(downstream) , N-Nym(Upstream) - Next Pseudonym, P-hop – Previous hop,N-hop – Next hop.

b) Route Reply

After node D finds out it is the destination node, it starts to prepare a reply message to the source node. D chooses a random number and computes a ciphertext showing that he is the valid destination capable of opening the trapdoor information. A session key is computed for data protection. Then he generates a new pair wise pseudonym between C and him. At the end, using the pair wise session key. it computes and sends the following message to C.

When C receives the above message from D, it identifies who the sender of the message is by evaluating the equation so he uses the right key to decrypts the cipher text, then it finds out which route this RREP is related to according to the route pseudonym and sequence number. C then searches its route table and modifies the temporary entry and sends the message to B. Other intermediate nodes perform the same operations as C does. Finally, the route reply is sent back to the source node S.

S decrypts the cipher text using the right key S is ensured that D has successfully opened the route request packet, and the route reply is really originated from the destination node D. S also computes the same session key S has successfully found a route to the destination node D, and the route discovery process is finished with success.

c) Unobservable Data Packet Transmission

The source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of pseudonyms and keys. Data packets from S must traverse A, B, and C to reach D. The data packets sent by S.

A receiving the message from S, A knows that this message is for him according to the pseudonym. After decryption using the right key, A knows this message is a data packet and should be forwarded to B according to route pseudonym. Hence, he composes and forwards the packet to B. Other intermediate nodes further forward the data packet until it reaches the destination node D. Finally data packet reached a node D. This is depends upon route table entry D knows himself is the destination of this packet.

d) Unobservability Scheme using Nonce :

A nonce, in information technology, is a number generated for a specific use, such as session authentication. In this context, "nonce" stands for "number used once" or "number once. "It is some value that varies with time, although a very large random number is sometimes used. A nonce can be a time stamp, a visit counter on a Web page, or prevent the unauthorized replay or reproduction of a file. An initialization vector (IV) is a nonce used for data encryption. The IV, used only once in any session, prevents repetition of sequences in encrypted text. Identifying such repetitions can help an attacker break a cipher.

In security engineering, nonce is an arbitrary number used only once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. A nonce may be used to ensure security for a stream cipher. Where the same key is used for more than one message then a different nonce is used to ensure that the keystream is different for different messages encrypted with that key. Often the message number is used. To ensure that a nonce is used only once, it should be time-variant , or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value. Some authors define pseudo randomness (or unpredictability) as a requirement for a nonce. Nonces are used in proof of work systems to vary the input to a cryptographic hash function so as to obtain a hash for a certain input that fulfils certain arbitrary conditions. In doing so, it becomes far more difficult to create a "desirable" hash than to verify it, shifting the burden of work onto one side of a transaction or system.

C. Attacks in MANET

There are different kinds of Attack in MANET like Eaves dropping, Wormhole, Blackhole, Denial of service etc. Attacker corrupts the route request packets and changes its content. Wormhole attack is occurred at the higher level. So, the detection becomes more complex.

A MANET provides network connectivity between mobile nodes over potentially multihop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing

states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: *routing attacks* and *packet forwarding attacks*, based on the target operation of the attacks.

1) An Overview of Attacks in MANETs

An ad hoc network nature is the main cause for making it more vulnerable to wireless attacks. Ad hoc nodes are wireless in nature that makes it prone to attacks including Eavesdropping, Black Hole, Wormhole, denial of service etc. An autonomous feature of ad hoc nodes is responsible for the motivation of attacks. The nodes are free to move anywhere in a wireless environment and can join or leave any network at any time. These nodes are not fully secured and can be compromised, confined or hijacked by any attackers. There is no central authority and it is assumed that all participating nodes are cooperative in nature. Many algorithms were proposed to ensure the node co-operation. The major aim of the attacker is to destroy the cooperativeness of the ad hoc nodes.

2) Types of Attacks in MANETs

A secured MANET system can be achieved only by preventing routing protocol attacks. Several routing protocol attacks are identified through a literature survey. Such attacks are discussed in this section that affects the routing process in ad hoc wireless network. A rushing attacker corrupts the route request packets, modifies the content of the node cache and rushes the packet to neighbor node. The reactive protocol broadcast a single route request at a time. Suppose the route request broadcasted by rushing attacker reaches the destination first, and then all routes discovered include a route only through the attacker. The routing table poisoning involves in sending false routing updates that result in network congestion and network partition. In blackhole attack, malicious nodes deliberately advertise itself as it has the shortest path to reach the receiver. After obtaining the path, it will drop all data packets without forwarding. Misbehavior of nodes result in Sybil attack in which a single node dishonestly represents the numerous identities by thieving true identities. A stealthy attack result in packet dropping and it is a combination of attacks like misrouting, colluding collision, and power management and identity entrustment. The stealthy attack does not allow a packet to reach the receiver. A malevolent node makes the neighboring node to trust that it correctly forward packet to the next hop.

3) Wormhole Attack

The wormhole is one of the challenging attacks in the ad hoc routing in which two malicious nodes forms a tunnel with high transmission connectivity referred as a wormhole tunnel. The wormhole tunnel may be wired or wireless form or an optical link. As soon as malicious nodes launch a wormhole link they start gathering the wireless data and forward it to one another. It is then relay the packets over the wormhole tunnel to some other location. The legitimate data packets are relayed to some other place in the network and malicious nodes makes other nodes to believe that they are immediate neighbors. By doing so, it gains the entire communication channel through them. The wormhole attack affects both the proactive and on demand routing protocols. In the presence of wormhole, genuine nodes in the network do not predict the original network formation. This causes severe damage in networks that is based on localization schemes and it may lead the genuine nodes to take wrong decisions. It is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do and where and when. The wormhole attack is invisible at the higher layer and therefore, two end points of the wormhole are not visible in the route in which detection becomes much more complex. The wormhole nodes result in denial of service as it discards all data packets instead of forwarding. In the wormhole attack, a malevolent node gets a data packet at one end of the network and tunnels or replays them into the other end of a network and this process is repeated. The most dangerous thing in this attack is that the attacker becomes invisible at the higher layers. The wormhole attacker drops the packets or selectively forwards packets so that it cannot be detected. The wormhole attacker can launch its attack even in the network with better security in terms of authenticity and confidentiality. The wormhole locates the attacker in the central part of the network and thus, the attacker uses this location in several ways. The result of wormhole attack is that it discards the data packets instead of forwarding these data packets and thus resulting in a denial of service attack or particularly discarding the data packets. These are some of the possible dangerous attacks in MANET. Therefore, we present a proficient technique for the detection of the wormhole attack.

The following figure gives the idea about the wormhole attack. It gives the brief idea about the attacker nodes, how it makes the tunnel to the other node.

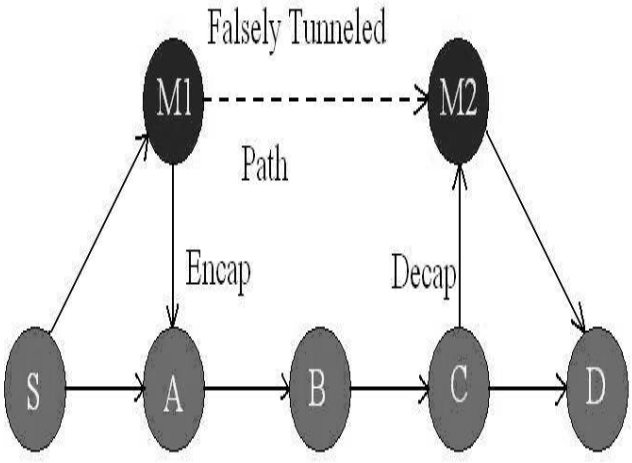


Fig 1: wormhole Attack

Here, M1 and M2 are the attacker nodes. Source sends the route request to the M1 node and M1 makes the tunnel to the other node i.e M2. M2 knows the destination node. So, it searches the destination and it corrupts the other route request signal. The attacker reaches the destination and it gives the advertisement to other nodes. I am having the shortest path, so, all the nodes are started to transfer the data through these nodes. The data transfer through the honest nodes should be stopped. The attacker nodes will not transfer data to destination node; it drops or transfers to somewhere

V. CONCLUSION

In this paper, we analyzed the wormhole attack. This is one of the Higher Layer Attack. This is major issue of the MANET is to detect and prevent the wormhole attack. Two Malicious

nodes are entered into the network and form the tunnel between the nodes. Attacker node received all the packets, drops the packets into some other location.

In this project, an Unobservable routing protocol USOR based on group signature and ID based cryptosystem for Ad hoc network is implemented. The design of USOR offers strong privacy protection-Complete unlinkability and content unobservability for adhoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The implementation of the protocol and its performance shows satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

REFERENCES

[1] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, IEEE/ACM Trans, Dec 2001, Topological detection on wormholes in wireless ad hoc and sensor networks, 1787 - 1796.

[2] D. Boneh and M. Franklin, Lecture Notes in Computer Science in Advances in Cryptology – Crypto'01, 2001, Identity-based encryption from the Weil pairing, 213–229.

[3] J. Kong and X. Hong, in Proc. ACM MOBIHOC, 2003, ANODR: anonymous on demand routing with untraceable routes for mobile ad - hoc networks ," 291–302.

[4] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, IEEE Conference on Local Computer Networks, 2004, Anonymous secure routing in mobile ad-hoc networks, 102–108.

[5] L. Song , L. Korba, and G. Yee, ACM Workshop on Security of Ad Hoc & Sensor Networks, 2005, AnonDSR : efficient anonymous dynamic source routing for mobile ad-hoc networks, 33–42.

[6] S. Seys and B. Preneel, IEEE International Conference on Advanced Information Networking and Applications, 2006, ARM: anonymous routing protocol for mobile ad hoc networks, 133–137.

[7] D. Sy, R. Chen, and L. Bao, IEEE Conference on Mobile Ad-hoc and Sensor Systems, 2006, ODAR: on-demand anonymous routing in ad hoc networks, 133-137.

[8] J. Ren, Y. Li, and T. Li, in Proc. IEEE MAS, 2009, Providing source privacy in mobile ad hoc networks"
332 - 341.

[9] J.Sel, IEEE Areas Commun,vol. 29, no. 10, 2011, Privacy- preserving location- based on- demand routing in MANETs, 1926–1934.

[10] K. E. Defrawy and G. Tsudik, IEEE Trans. Mobile Comput., Vol. 10, no. 9, 2011, ALARM: anonymous location-aided routing in suspicious MANETs, 1345–1358.

[11] Reshmi Maulik and Nabendu Chaki, International Journal of Computer Information systems and Industrial Management Applications, Vol. 3, 2011, A Study of Wormhole Attacks in MANET, 271 - 274.

[12] Zhiguo Wan, Kui Ren, and Ming Gu, Vol. 11, No.5, May 2012, USOR : An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks, 1922 – 1927.

[13] T. Sakthivel and R.M. Chandrasekaran, European journal of Scientific Research, Vol.76 ,No.2, 2012, Detection and Prevention of wormhole Attacks in MANETs using Path Tracing Approach, 240-247.