Anonymity, Unlinkability and Unobservability in Mobile Ad Hoc Networks

Akhilamol Vijayan, Tony Thomas

***Abstract*—Mobile ad hoc networks have the features of open medium, dynamic topology, cooperative algorithms, lack of centralized monitoring etc. Due to these, mobile ad hoc networks are much vulnerable to security attacks when compared to wired networks. There are various routing protocols that have been developed to cope up with the limitations imposed by the ad hoc networks. But none of these routing schemes provide complete unlinkability and unobservability. In this paper we have done a survey about anonymous routing and secure communications in mobile ad hoc networks. Different routing protocols are analyzed based on public/private key pairs and cryptosystems, within that USOR can well protect user privacy against both inside and outside attackers. It is a combination of group signature scheme and ID based encryption scheme. These are run during the route discovery process. We implement USOR on ns2, and then its performance is compared with AODV.**

***Index Terms*— Anonymity, routing protocols, security, unlinkability, unobservability.**

I. Introduction

Mobile Ad Hoc Network [MANET] can be outlined as a collection of large number of nodes that form a network that is temporary. People and vehicles can be inter networked in areas have no pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate nodes to communicate with each other. Every node in the network will forward packets to other nodes, so each node can act as both router and as hosts. In these two situations, all the nodes in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. Since MANET is vulnerable to a lot of security attacks [1], so it is essential to provide privacy for secure routing.

The routing protocol for wired networks cannot be used for mobile ad hoc networks because of the mobility of the networks. The network topology in a MANET changes according with time. Therefore, it provides new challenges for routing protocols in MANET but the traditional routing protocols are not suitable for MANET. Most of the schemes fail to protect all content of packets from attackers, so the attacker can obtain information. By using this information the attacker can relate two packets. The various privacy related notations in communication networks are anonymity, unlinkability and unobservability.

A. Anonymity

There are two types of anonymity [2] data anonymity and connection anonymity. Data anonymity is filtering any identifying information out of the data that is exchanged in a particular application. Connection anonymity is hiding the identities of source and destination during the actual data transfer. Here, we give importance to connection anonymity. Nodes in MANET do not reveal its identity within the network and outside the network. All the nodes are anonymous to each other (they do not know about each other). Pfitzmann and Hansen defined anonymity 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 mobile ad hoc network 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. A sender is identifiable when we get information that can be linked to him.

B. Unlinkability

It provides security at the time of data transfer, it hides the message. It will not show what kind of data or information is transferred between the two nodes. Suppose two messages and their signatures are given, we can't tell if the signatures were from the same signer or not.

C. Unobservability

In unlinkability, it hides only the data. It will not hide the packet type and packet header information. But unobservability [2] protects content of the packet, such as packet header and packet type etc. To achieve unobservability, a routing scheme should provide unobservability for both the content and traffic pattern.

USOR [3] achieves anonymity by Anonymous key establishent. This key establishment is based on group signature scheme that is, the signature doesn't reveal the signer's identity but anybody can verify its identity. Firstly each node obtains a group signature signing key and ID based private key from an offline key server. Then this anonymous key establishment process is performed to construct secret session

Akhilamol Vijayan is with the ECE department,Vivekanandha Engineering College for Women,Sankari,Salem,Tamilnadu,India; e-mail: akhilave88@ gmail.com.

Tony Thomas was with the Department of mathematics, IIT,Kanpur. He is now with the School of Computer Science and Information Technology, IIITM-Kerala, Thiruvananthapuram, India e-mail:tony.thomas@iiitmk.ac.in.

978-1-4799-3358-7/14/$31.00 ©2014 IEEE

IEEE Advancing Technology for Humanity

keys. Then to achieve unlinkability and unobservability USOR uses ID based encryption [4] in the route discovery process.

In this paper, we analyzed different public/private key pairs (one-time or long-term) and different public key crypto-systems. The contribution of this paper include, 1) Analysis of different anonymous routing schemes 2) Comparison of various routing protocols 3) Implemented USOR on ns2 and compared its performance with implementation of AODV.

In the next section, we discuss related works, in that different routing schemes in mobile ad hoc networks are analyzed and compared. Section III shows the privacy preserving routing scheme, where USOR protocol is explained. Section IV shows the experimental results and performance evaluation based on packet delivery ratio and packet drop. Finally, we conclude the paper.

II. Related Works

A number of privacy preserving schemes have been proposed in the recent years and they provide different level of privacy. They can be classified into five categories; Based on one-time public/private key pairs, long-term public/private key pairs, public key cryptosystems, pairing based cryptosystems and also based on public key cryptography and group signature scheme.

Many of these schemes depend on public key cryptosystems (PKC) for obtaining anonymity and unlinkability in routing. Asymmetry of these public key cryptosystems offer better support for privacy protection, but expensive PKC operations bring vital computation overhead. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption.

A. Based on one-time public/private key pairs

In 2003 Jiejun Kong and Xiaoyan Hon**,** proposed ANODR, [5] an anonymous on-demand routing protocol for mobile ad hoc networks. ANODR uses onion routing for route discovery and private/public key for obtaining anonymity. It offers sender, receiver, and route anonymity as well as sender and receiver unobservability. The route discovery method establishes an on-demand route between its source and destination. The disadvantages of ANODR are, 1) Each forwarding node has to generate a fresh public/secret key pair for each RREQ message it forwards. 2) For a node to decide whether it has to forward a RREP or not, it has to decrypt it with every private key. Each node encrypts the routing information with its own secret key during the route discovery so that the source and destination does not know the whole route.

In 2004, Bo Zhu*,* Feng Bao Zhiguo Wan*,* Mohan S. Kankanhalli, and Robert H. Deng, [6] proposed the Anonymous Secure Routing (ASR) protocol that can provide anonymity, that is Identity Anonymity and Strong Location Privacy, and at the same time ensure the security against various passive and active attacks. They have conducted detailed analysis on how anonymity and security can be achieved, and at the same time showed advantages compared to previous works. ASR makes use of one-time public/private key pairs to achieve anonymity and unlinkability. The disadvantage is that every forwarding node has to generate a fresh public/secret key pair for RREQ message it forwards, which affects the efficiency.

In 2005 L. Song, L. Korba, and G. Yee [7] proposed AnonDSR which uses one-time public/secret key pair consist of three protocols which is used to create a secret key and random Nonce between source and destination. AnonDSR uses this secret key to create a trapdoor and employ an anonymous onion routing. At last, the source and destination use their session keys shared with intermediate nodes to encrypt all communications with the cryptographic onion method. It provides an end to end encryption protection.

In 2006, Stefaan Seys and Bart Preneel [8] described a novel anonymous on demand routing scheme for MANETs. ARM is to reduce computation burden on one-time public/private key pair generation. This protocol hides routes in the network, both against a passive global adversary and nodes inside the network. A probabilistic padding and a TTL scheme are used; nodes inside the network will not be able to determine whether they received a message from the source or destination. Nodes that participate in hiding process only need to decrypt and encrypt the short message header using their broadcast keys. One of the disadvantages is that packets are not protected as a whole.

B. Based on long-term public/private key pairs

Azzedine Boukerche, Khalil El-Khatib,Larry Korba, Li Xu, [9] proposed a distributed routing protocol which guarantees security, anonymity and high reliability. SDAR use long-term public/private key pairs at each node for anonymous communication. SDAR introduces the notion of trust management system. The purpose of this system is to motivate the nodes to help each other and relaying data traffic. SDAR also identifies the malicious nodes, and avoids the nodes during the route establishment. The identification of malicious nodes makes it easy to take them out of the network, thereby increasing the route's security and reliability. It is more scalable to network size, but requires more computation effort. It guarantees security, anonymity and high reliability but route discovery is inefficient. But SDSR [10] provides mechanism for secured route discovery, even under adversarial condition. It uses a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication.

Xiaoqing Li, Hui Li, Jianfeng Ma, Weidong Zhang [11] provide a valid method to detect malicious nodes and also provide a trustworthy protection over the whole network. In this paper, they introduce a localized trust management which can primarily remove malicious nodes, and propose an efficient anonymous routing protocol. The node that participates in the protocol encrypts entire message with trust key and says Hello to its ancestor within expiration time, like this the malicious node can be detected and isolated from the network. This protocol employs onion routing algorithm to

achieve the anonymity. Hence, an anonymous and secure route path can be established. Additionally, it has better characteristic for defending against many attacks. It does not offer complete unlinkability or unobservability since data packets and control packets are linkable and distinguishable.

C. Public key cryptosystems

Denh Sy, Rex Chen and Lichun Bao [12] proposed ODAR, an On-Demand Anonymous Routing protocol for wireless ad hoc networks. ODAR provides complete anonymity of nodes, links and source routing paths using bloom filters. The use of bloom filters is to provide ODAR storage, processing and communication efficiencies. ODAR provides only identity anonymity but not unlinkability, and RREQ/RREP packets are not protected with session keys. A key management mechanism is used to provide strong anonymity. This is a reactive on-demand routing control algorithm and follows the usual route request and reply mechanisms.

D. Pairing-based cryptosystems

MASK [13] is based on a special type of public key cryptosystem called pairing based cryptosystem, to enable anonymous communication thereby thwarting possible traffic analysis attacks. MASK requires a trusted authority to generate sufficient pairs of secret points, corresponding pseudonyms and cryptographic parameters. This proposed an anonymous neighborhood protocol that permits neighboring nodes to authenticate each other while not revealing their identities. The basic idea of MASK is the anonymous neighborhood authentication based on the dynamically changing pseudonyms of nodes instead of their real identifiers. It provides sender and receiver anonymity as well as relationship anonymity of the sender and receiver. Due to the concept of pairing, there is low computation overhead and high routing efficiency. MASK can stand up to a wide range of attacks including message coding attack, flows recognition attack etc. Adversaries cannot track a selected packet back to its source or trace it forward to its destination. One of the disadvantages is that MASK does not always use the best path and also introduce extra delay and delay jitter. MASK is vulnerable to key pair depletion attacks.

E. Based on public key cryptography and group signature

In 2011, Karim El Defrawy, and Gene Tsudik [14] proposed ALARM, it makes use of public key cryptography and the group signature to preserve privacy. The group signature has good privacy preserving feature, in this everyone can verify a group signature but cannot identify who is the signer. But ALARM leaks a lot of sensitive privacy information such as network topology, location of every node, etc. By using this group signature ALARM construct one-time pseudonyms that are used to identify nodes at certain locations. This works with any group signature scheme and any location based protocol that can be used to route data between nodes. Even if a portion of the nodes are stationary, or if the speed of movement is not very high the node privacy is preserved. ALARM is viable, security and privacy requirements must be reconciled and resistance to both outsider and insider attacks is needed.

Table 1. Shows the comparison of different routing protocols in the mobile ad hoc environment.

TABLE 1

COMPARISON OF VARIOUS ROUTING PROTOCOLS

Protocols	Anon-ymity	Unlinka-bility	Traffic Unobser vablity	Content Unobser-vability
ANODR	Yes	Yes	Yes	No
ASR	Yes	No	No	No
ARM	Yes	No	Yes	No
Anon DSR	Yes	No	Yes	No
SDAR	Yes	No	No	No
ODAR	Yes	No	Yes	No
MASK	Yes	No	Yes	No
ALARM	Yes	Yes	Yes	No
USOR	Yes	Yes	Yes	Yes

III. PRIVACY PRESERVING ROUTING SCHEME

In USOR protocol control and data packets are not identifiable by attackers. By using symmetric decryption the valid node can distinguish packets. Each node establishes a key with its neighbor; by using this key it encrypt the packet. It uses two types of keys a group key and a pair wise key to support broadcast and uncast. USOR has two phases 1) Anonymous key establishment 2) Route discovery.

1) Anonymous key establishment

In this phase each node anonymously establishes a set of session key with its neighbors. Every node communicates with its neighbors within its radio range by using the private signing key and private ID based key. The intuition of the USOR protocol is that if a node establishes a key with its neighbor, then it can use that key to encrypt the whole packet for the corresponding neighbor.

By doing the trial decryption the receiving node can distinguish whether the encrypted packet is intended for itself or not. Anonymity can be preserved in this phase. The two nodes establish the key without knowing the other party.

2) Route discovery

This phase preserve the unlinkability and unobservability based on the keys established in the previous phase. This phase comprises of route request and route reply. Route request is flood through the whole network, but the route reply messages are sent back to the source node as unicast.

Route discovery uses the pseudonymity approach and Nonce; by using this, the unobservability can be achieved. Nonces are used once and never reused. Pseudonyms are calculated from the Nonce, so both the Nonce and pseudonyms changed every time. The attacker can eavesdrop every transmission, but impossible to decrypt the message without knowing the encryption key. The attacker never get the idea of the type of packet being transmitted and cannot relate different packet type.

The Nonce is updated each time after it is used, so there is no linkage between the pseudonyms which are computed from Nonce. Nodes having valid session keys can recognize pseudonyms and decrypt the data. Each nodes next-hop node and previous-hop node on the route establish session key, so no one cannot identifies the real identities. As a result USOR offers content unobservability.

In 2013 S.Balaji, Manicka Prabha. M proposed an Unobservable Secure Proactive Routing Protocol for Fast and Secure transmission using BATMAN [15]. The BATMAN routing protocol provides a secure and fast transmission of data and it maintains only the best hop. But the disadvantage is that paths with better QoS may not be chosen and routing decisions are made without any awareness of the resources available and requirements needed by applications.

IV. Implementation and Performance Evaluation

In the simulation process 50 nodes are randomly distributed within a network field of size 1350m×1250m. Each mobile node can move within this field. The session keys are updated every 40 seconds and each update involves an anonymous key establishment. We evaluate the performance of USOR in terms of packet delivery ratio and packet drop by comparing it with the standard AODV.

Fig.1. shows the packet delivery ratio of AODV and USOR. Packet delivery ratio is the ratio of the number of delivered data packet to the destination, which illustrates the level of delivered data to the destination.

Fig. 2 shows the packet drop of AODV and USOR. Packet drop occurs when one or more packets of data travelling across a computer network fail to reach their destination. AODV has the highest packet delivery ratio, the packet delivery ratio decreases as nodal speed increases. The difference between USOR and AODV on packet delivery ratio is less than 10%. Route disruption leads to packet drop. USOR have better result in packet drop compared with AODV.

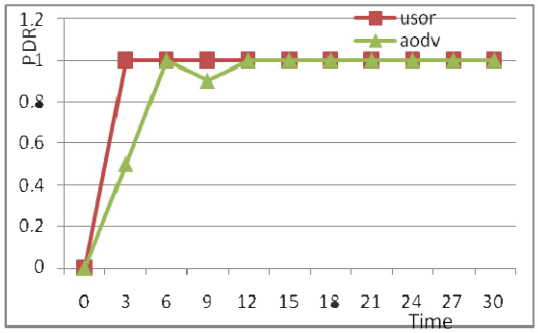


Fig.1. Packet delivery ratio

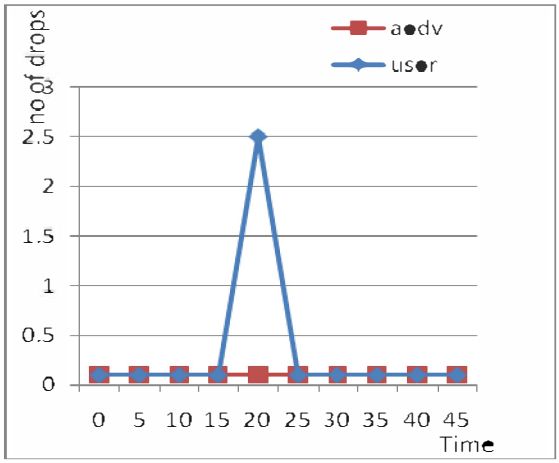


Fig.2. Packet drop

V. Conclusion

In this paper, we have carried out a survey about various routing protocols. Only the USOR protocol preserve anonymity, unlinkability and unobservability by using the group signature and ID based encryption scheme. We implemented USOR on ns2 and the performances are evaluated in terms of packet delivery ratio and packet drop. It shows good performance when compared with AODV and other routing protocol.

Future work along this direction is how to prevent wormhole attack which is a serious routing attack. By using path tracing algorithm we can detects wormhole attack and isolates the affected node from the networks. This algorithm is very easy and does not require any special hardware. We think the path tracing algorithm will work effectively in mobile ad hoc networks.

REFERENCES

[1] P.Karthikkannan, K.P.Lavanya Priya "Reduction of delays in reactive routing protocol for unobservable Mobile Ad-Hoc Networks", *IEEE Conference Publications*, 2013, pp. 463-467.

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

[3] Zhiguo Wan, Kui Ren, and Ming Gu, "USOR: An Unobservable On demand Routing protocol for Mobile Ad hoc network", *IEEE transactions on wireless communications*, vol. 11, no. 5, pp. 1922-1933, may 2012.

[4] D. Boneh and M. Franklin, "*Identity-based encryption from the Weil pairing*," in Advances in Cryptology–Crypto'01, Lecture Notes in Computer Science, vol. 2139, 2001, pp. 213–229

[5] J. Kong and X. Hong, "ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. *ACM MOBI-HOC*'03, pp. 291–302.

[6] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. Kankan Halli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 *IEEE Conference on Local Computer Networks*, pp. 102–108.

[7] L. Song, L. Korba, and G. Yee, "AnonDSR: 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

[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] 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.

[10] L. Vijayanand R.K. Negesh "SDSR: A Secure on-Demand Routing Protocol for MANETS" *Third International Conference on Sustainable Energy and Intelligent System,*VCTW, Tiruchengode, December, 2012.

[11] Xiaoqing Li, Hui Li, Jianfeng Ma, Weidong Zhang "An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks" *IEEE Conference Publications*, 2009, pp. 287-290.

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

[13] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *2005 IEEE INFOCOM*.

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

[15] S. Balaji, Manicka Prabha. M "UOSPR: UnObservable Secure Proactive Routing Protocol for Fast and Secure transmission using B.A.T.M.A.N, *IEEE Conference Publications*, March 2013, pp 1-4.