Performance of Comparison between AODV and Secured Protocol

J.Vani
M.E Communication System
Dept. Electronics and
Communication Engineering
GKM College of Engineering
And Technology
Chennai-63, India

AL.Visalatchi
Assistant Professor,
Electronics and
Communication Engineering
GKM college of Engineering
and Technology
Chennai-63, India

ABSTRACT

In mobile ad hoc networks packets are relayed over multiple hops to reach their destination. Due to the features of open medium, dynamic topology, cooperative algorithms, lack of centralized monitoring and management point mobile ad-hoc networks are much more vulnerable to security attacks when compared to the wired networks. A number of secure routing schemes have been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. The main objective of the project is to provide an anonymous routing and secure communications in mobile ad hoc networks. Therefore a new on demand routing protocol called Unobservable Secure On demand Routing protocol (USOR) is proposed to offer complete unlinkability and content unobservability for all types of packets. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers. USOR is implemented by using ns2, and evaluate its performance by comparing with AODV.

Keywords

Routing protocols,security, anonymity, unobservability, ad hoc networks, unlinkability.

1. INTRODUCTION

Privacy protection in routing of MANET has interested a lot of research efforts. Mobile ad hoc networks play an increasinglyimportant role in many environments and applications, especially, in critical settings that lack fixed network infrastructure. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. Compared to the wired networks, mobile ad-hoc networksare much more vulnerable to security attacks. The existing routing protocols provides both security and privacy features, including node authentication, data integrity, anonymity and partial unlinkability. Apart from this the security parameter which is not still considered in communication networks unobservability as discussed in [1]. Unobservability of an IOI (Item of Interest) is the State that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects. Privacy protection in routing of MANET has interested a lot of research efforts. A number of privacy-preserving routing schemes have been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET, most of them exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which breaks unlinkability and may lead to source trace back attacks. Meanwhile, unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to achieve complete unlinkability and unobservability.

Among these requirements unobservability is the strongest one in that it implies not only anonymity but also unlinkability. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence further refine unobservability into two types: 1) Content Unobservability, referring to no useful information can be extracted from content of any message; 2) Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. This paper will focus on content unobservability, which is orthogonal to traffic pattern unobservability, and it can be combined with mechanisms offering traffic pattern unobservability to achieve truly unobservable communication. The major mechanisms to achieve traffic pattern unobservability include MIXes [3] and traffic padding [2].

In this paper, an efficient privacy-preserving routing protocol USOR is proposed that achieves content unobservability by employing anonymous key establishment based on group signature. The setup of USOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme like [4]. The unobservable routing protocol is then executed in two phases. First, an anonymous key establishment process is performed to construct

Secret session keys.

2. RELATED WORK

Several methods for withstanding eavesdropping and other kinds of traffic analysis have been investigated. Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks.

A number of secure routing schemes have been brought forward. However, existing anonymous routing protocols

mainly consider anonymity and partial unlinkability in MANET, most of them effort asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection.

The ANODR scheme proposed by Kong et al. [5] is the first one to provide anonymity and unlinkability for routing in ad hoc networks.ANODR uses the onion routing for the route discovery.ASR scheme proposed by Zhu et al [6] provide additional property of anonymity and also provide stronger privacy protection than ANODR. In ASRAnonymous data transmission is similar to route pseudonym i.e., to add small information along with the data packet.

AnonDSR proposed by Song et al [8] provide strong security and anonymity protection and better scalabity. The design includes creating sharing the secret key and random nonce between source and destination. SDAR [10] and ODAR [11] uses long term public/private key pair. They are more scalable to network size but require more computation effort. ODAR provides only identity anonymity but not unlinkability. SDAR has three issues namely trapdoor issue, scalabity issue, security issue.

ARM [7] uses shared secrets between source and destination for verification. It considered reducing computation burden on one-time public/private key pair generation. An anonymous location-aided routing scheme ALARM [14] makes use of public key cryptography and the group signature to preserve privacy. The group signature has a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaks quite lot sensitive privacy information like network topology and location of every node.Similar to ALARM, PRISM [15] also employs location information and group signature to protect privacy in MANETs.To summarize, existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which break unlink ability and may lead to source trace back attacks. Another drawback of most previous schemes is that they rely heavily on public key cryptography, and thus incur a very high computation overhead.

3. AN UNOBSERVABLE ROUTING PROTOCOL SCHEME

Privacy-preserving routing is crucial for some ad-hoc networks that require stronger privacy protection. In this paper an efficient privacy-preserving routing protocol USOR is proposed. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. USORachieves content unobservability by employing anonymous key establishment based on group signature. Each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme then the unobservable routing protocol is then executed. The project provides a thorough analysis of existing anonymous routing schemes and demonstrates their vulnerabilities. It proposes USOR, the first unobservable routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications. Detailed security analysis and comparison between USOR and other related schemes are presented in the paper. Giving unobservable secure is for, to protect all parts of a packet's content, and it is independent of solutions on traffic pattern Unobservability, to protect privacy in ad-hoc networks, to define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks, to propose an unobservable secure routing scheme USOR to offer complete unlinkability and content Unobservability for all types of packets.

There are four modules in this system: 1) Attack Model,2) Key Establishment, 3) Route Discovery and 4) Performance Analysis.

3.1Attack model

In Attack model formulate an adversary model in the network. Adversaries are intruders in the network they do false things against the protocol. The adversary model here for monitoring the network activities such as record data, time and size of the packet sent over the network also it observes the source and destination nodes id for disrupting the packet transmission. The attack used in the proposed method is black hole attack. In this type of attack, a malicious node advertises itself as having the shortest path to all nodes in the network (e.g. the attacker claims that it is a level-one node). The attacker can cause DoS by dropping all the received packets. Alternately, the attacker can monitor and analyse the traffic to find activity patterns of each node. Sometimes the black hole becomes the first step of a man-in-the-middle attack.

3.2. Key establishment

The key establishment protocol is designed following the principal of KAM [21], which employs Diffie-Hellman key exchange and secure MAC code. It can effectively prevent replay attacks and session key disclosure attack and meanwhile, it achieves key confirmation for established session keys. By providing content protection can achieve unlinkability and unobservability. Thus by establishing an anonymous key for each node with in the network can achieve completed anonymous in a network. In this paper, Elliptic curve Diffie Hellman key exchange algorithm is used for establishing anonymous key for all nodes in an unobservable manner. Use group signature technique for preserving privacy.

3.3Route discovery

The route discovery process comprises of route request and route reply. Source node uses an anonymous key to encrypt whole control packet and flood across a network. Intermediate nodes try to decrypt the received packets as a trial and error. If not it's just add its header information and do the same process as source node. Only the intended destination node can decrypt and response with acknowledgement.

3.4 Performance analysis

Let us focus on the performance of this routing protocol and evaluated the performance using ns2. To analysis the performance of this protocol is based on packet delivery ratio, packet delivery latency and normalised control bytes.

4. DISCUSSION

The fundamental difference between USOR and ANODR or AnonDSR is that USOR relies on established keys between neighboring nodes to achieve privacy protection, while the other two schemes depend on onion encryption and end-to end security. Consequently, per-hop protection in USOR can able to provide complete unlinkability and unobservability efficiently, but ANODR and AnonDSR fail to protect link

ability or observability of messages. Another of USOR over ANODR is the constant size of routing packets. This makes USOR more advantageous as the attacker cannot obtain private information from packet size, while ANODR has to deal with this issue by padding packets to the same size. User anonymity is implemented by group signature which can be verified without disclosing one's identity. Group signature is used to establish session keys between neighbouring nodes , so that they can authenticate each other anonymously. And subsequent routing discovery procedure is built on the top of these session keys.

Hence it is easy to see that USOR fulfils the anonymity requirement under attacks. Based on content unobservability provided by USOR, traffic padding can be introduced into the network for traffic pattern unobservability.Node compromise is easy for the adversary and highly possible in ad hoc networks; hence it is crucial for a privacy-preserving routing protocol to withstand security attacks due to node capture. In this case, privacy information leakage is unavoidable due to secret exposure; while in the routing protocol can protect user privacy against serious node compromise. Suppose a node is compromised by an attacker, his private signing key and ID-based encryption key are disclosed to the attacker. The attacker now is able to establish keys with neighboring nodes, but only the following information can be obtained by the attacker: 1) the type of a received packet;2) data/RREP packets sent to/via the compromised node; 3) headers of packets relayed by the compromised node; 4) RREQ packets sent from the compromised node's neighbors.

The attacker is not able to gain more beyond this information. From this information, he cannot infer: 1) the location of the source/destination node; 2) real identities of source/destination node of the relaying packets; 3) source/destination node of the RREQ packets. That is, the privacy leakage due to node compromise is limited within the compromised node's neighborhood, and privacy information like identity and location is still well protected by USOR.

5. IMPLEMENTATION AND PERFORMANCE EVALUATIONS

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-encryption/decryption and two point multiplications. A detailed comparison on computation cost of existing schemes and USOR is showed in Table I. In this table, ignore symmetric operations as they are negligible compared to PKC operations.

TABLE I

COMPUTATION COST OF USOR AND EXISTING SCHEMES

	Computation cost †		
	Source	Destination	Intermediate
ANODR	KG+1P(1P)	1P	KG+2P(2P)
ASR	KG+1P(1P)	1P	KG+2P(2P)
ARM	KG+1P(1P)	L*P	1P
AnonDSR	KG+1P(1P)	$(L+1)$*P	1P
SDAR	KG+2P(2P)	$(L+1)$*P	KG+1P(1P)
ODAR	KG+1P(1P)	1P	0
ARMR	KG+3P(3P)	3P	4P
PRISM	KG+3P(3P)	3P	0
ALARM	KG+2P(2P)	2P	0
USOR	4P(3P)	4P(3P)	P

Numbers in brackets are computation complexity with pre-computation. L is the hops from the source to the destination, KG denotes public key generation, P denotes public key operations, e.g., PKC encryption/decryption, ECC pairing.

TABLE II

PARAMETERS ON CRYPTOGRAPHIC OPERATIONS AND EXPERIMENT SCENARIOS

1024-bit ID-based Enc	**22ms**
1024-bit ID-based Dec	**17ms**
Group Signature Generation	**24ms**
Group Signature Verification	**26ms**
Point Multiplication	**3ms**
1024-bit Pairing	**8.6ms**
Simulation Time	**600s**
Scenario Dimension	**1500m x 300m**
Wireless Radio Range	**250m**
Mobile Nodes Number	**50**
Average Node Speed	**0-10m/s**
Source-Destination Pairs	**20 random pairs**
Traffic Type	**CBR Traffic**
Frequency	**2 or 4 packets/s**
Wireless Bandwidth	**2Mbps**
Node Pause Time	**0s**
Key Update Interval	**40s**
Average Hops	**2.90**
Average Neighbors	**12.69**

6. PERFORMANCE OF COMPARISION BETWEEN USOR AND AODV

Implementthe USOR in ns2, and evaluate their performance by comparing with AODV (the standard implementation of ns-2.37). In this simulation, the scenario parameters are listed as in table In the simulation, 50 nodes are randomly distributed within a network field of size 750mx750m as such a rectangle field can make the number of hops between two nodes larger. Mobile nodes are moving in the field according to the random way point model, and we adopt the speed ranges used in [13] so that the average speeds range from 0 to 10m/s.

Evaluate the performance of USOR in terms of packet delivery ratio, packet delivery latency, and normalized controlbytes.

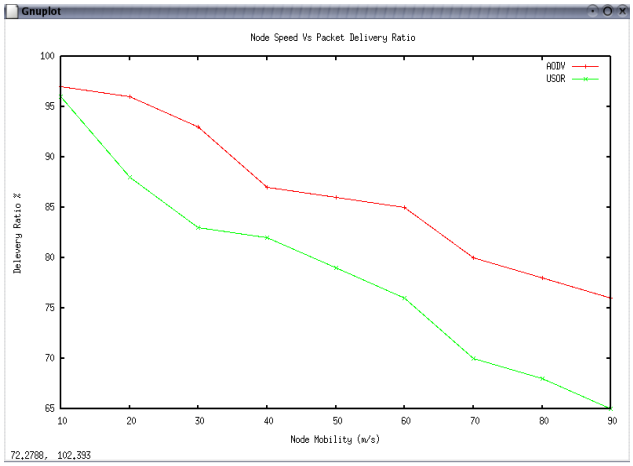

Fig.1.Xgraph for the comparison Of PDR With USOR and AODV

According to Fig.1, AODV has the highest packet

Delivery ratio. The packet delivery ratio decreases as nodal speed increases and traffic load becomes heavier. The biggest difference between USOR and AODV on packet delivery ratio is less than 10%. Apparently, the performance drop of both protocols when node speed goes up due to more frequent route disruption at higher speeds. Route disruption leads to packet drop and retransmission, and a new route has to be constructed before remaining packets can be sent out.

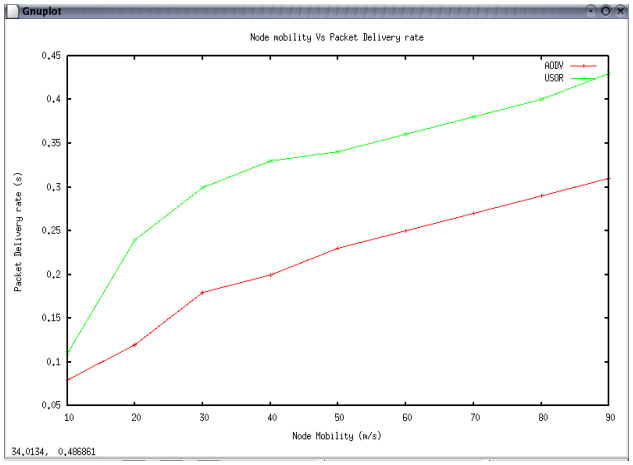

Fig.2.Xgraph for the comparison Of PDL With USOR and AODV

From Fig. 2, It is also seen that that AODV has the least deliverylatency, but the packet delivery latency difference between USOR and AODV is less than 100ms.Due to thesame reasons discussed above, non-optimal paths and localkey construction delay result in longer latency of USOR thanAODV.

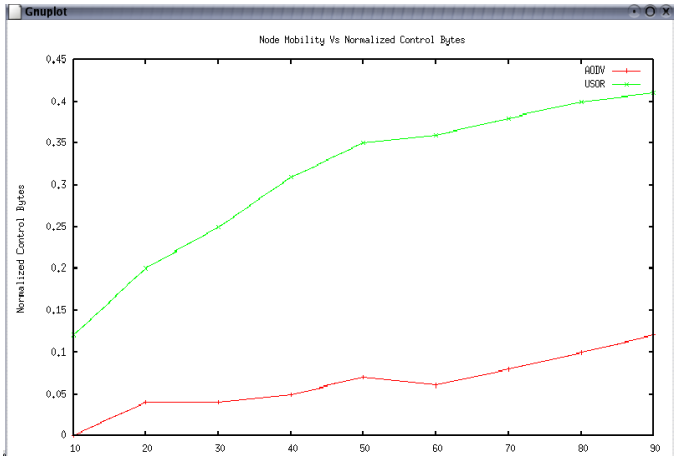

Fig.3.Xgraph for the comparison Of NCB With USOR and AODV

Fig.3 illustrates the routing cost for delivering a unit of data payload. It is not strange that USOR have to send more control packets than AODV. In AODV, 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. Since USOR exploit similar key management and route discovery approach, their normalized control bytes are very close.

But in the case of privacy protection USOR aheads AODV and all existing routing protocols by examing using the the entrophy based calculation since they use the group signature and ID based cryptosystem.

7. CONCLUSION AND FUTURE

Since nodes in mobile ad-hoc networks move dynamically, adversaries cannot conduct active attacks without knowing the location or identity of nodes. Therefore adversaries want to know the location or identity of the nodes to conduct active attack. Practically malicious nodes conduct traffic analysis passively first and later set active attack. However, to avoid such attacks nodes want to protect their location and/ or identity. Thus, anonymous communication becomes an essential factor in securing mobile ad hoc network routing. Most anonymous routing schemes proposed for MANET make use of public key cryptosystems to protect privacy. However, existing schemes provide only anonymity and unlinkability, while unobservability is never considered. An obvious drawback in existing schemes is that packets are not protected as a whole. To overcome this drawback an on demand route discover protocol called Unobservable Secure On-demand Routing (USOR) was proposed. The USOR is based on group signature and ID based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection such as complete unlinkability and unobservability for ad hoc networks.

There are many types of attacks such as wormhole attack, black hole attack, denial of service attack, man in the middle attack. In this project only the black hole attack is considered and the further enhancement of this project is done by considering the other attacks such as wormhole attack and DoS attack and analysis performance of each type of attacks.Moreover, security analysis is done to ensure anonymity, unlinkability and unobservability in mobile ad hoc networks.

8. ACKNOWLEDGMENTS

The authors would like to thank the Registrar Dr.K.O.Joseph, the Principal Dr.N.Ramaraj and the HOD Dr.D.Balasubramanian for their encouragement rendered in completion of this project with the constant technical support and invaluable guidance.

9. 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] D. Chaum, "Untraceable electronic mail, return , and digital pseudonyms," *Commun. of the ACM*, vol. 4, no. 2, Feb. 1981

[4] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-keymanagement for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

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

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

[7] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobilead hoc networks," in *Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications*, pp. 133–137.

[8] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymousdynamic source routing for mobile ad-hoc networks," in *Proc. 2005ACM Workshopon Security of Ad Hoc and Sensor Networks*, pp. 33–42.

[9] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR:anonymous routing protocol with multiple routes for communicationsin mobile ad hoc networks," *Ad HocNetworks*, vol. 7, no. 8, pp. 1536– 2009.

[10] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a securedistributed anonymous routing protocol for wireless and mobile ad hocnetworks," in *Proc. 2004 IEEE LCN*, pp. 618–624.

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

[12] J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc," in *Proc. IEEE MASS'09*, pp. 332–341.

[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-aidedrouting in suspicious MANETs," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358, 2011.

[15] K. E. Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in MANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1926– 1934, 2011.

[16] J. Han and Y. Liu, "Mutual anonymity for mobile peer-to-peer systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 8, pp. 1009–1019, Aug. 2008.

[17] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 464–475, 2011.