International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.2, March-April. 2013 pp-785-787 ISSN: 2249-6645

Privacy Protection Using Unobservablity and Unlink ability against Wormhole Attacks in Manet

N.Sugumar, [1] K.Jayarajan M.E, [2] R.Anbarasu, M.E[3]
[1]*Final Year M.E-CSE,*
[23] *Associate Professor Selvam College of Technology, Namakkal*

ABSTRACT: An efficient privacy-preserving routing protocol USOR that achieves content un-observability by employing anonymous key establishment based on group signature. The setup of USOR is simple: In privacy-preserving communications can largely be divided into two categories: cryptosystem-based techniques and broadcasting-based techniques. The cryptosystem-based techniques include mix-based systems and secure multiparty computation-based systems, originating from mix net and DC-net respectively. Broadcasting based schemes provide communication privacy by mixing the real messages with dummy packets so that it is infeasible for the adversaries to identify the real packets and track the message source. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination. This process is done by establishing session keys between two nodes. After verifying the signature between themselves, the anonymous key is established between these two nodes which mean the two nodes establish this key without knowing who the other party is. It can effectively prevent replay attacks and session key disclosure attack, and meanwhile, it achieves key confirmation for established session keys. This key establishment protocol uses elliptic curve Diffie- Hellman (ECDH) key exchange to replace Diffie-Hellman key exchange, and uses group signature to replace MAC code.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.

I. Introduction

Mobile computing is human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies.

Many types of mobile computers have been introduced
- Wearable Computer
- Personal Digital Assistant
- Smartphone
- Carputer
- UMPC

1.2 TECHNICAL AND LIMITATIONS OF MOBILE COMPUTING

1.2.1 Range & Bandwidth:

Mobile Internet access is generally slower than direct cable connections, using technologies suchas GPRS , 3G and 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

1.2.2 Security Standards:

When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

1.2.3 Power Consumption:

When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

1.2.4 Transmission Interferences:

Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

1.2.5 Potential Health Hazards:

People who use mobile devices while driving are often distracted from driving and are thus assumed more likely to be involved in traffic accidents.[3] (While this may seem obvious, there is considerable discussion about whether banning

mobile device use while driving reduces accidents or not.[4][5]) Cell phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health have been raised.

1.2.6 Human Interface with Device:

Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

II. Related Work

2.1 Anonymous Network Model

In this module, anonymous route is discovered between the nodes this information will not leak to others.This is adopted using session key and broadcast key generation by means of Key Generation Center(KGC).This anonymous connection is established by verifying signatures of the each node.

2.2 Secure Key Generation and Route Discovery Phase

This phase is a privacy-preserving route discovery process based on the keys established in previous phase.Similar to normal route discovery process, our discovery process 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.This performed based on the ID-based private key of every node.

2.3 Broadcast Key Distribution

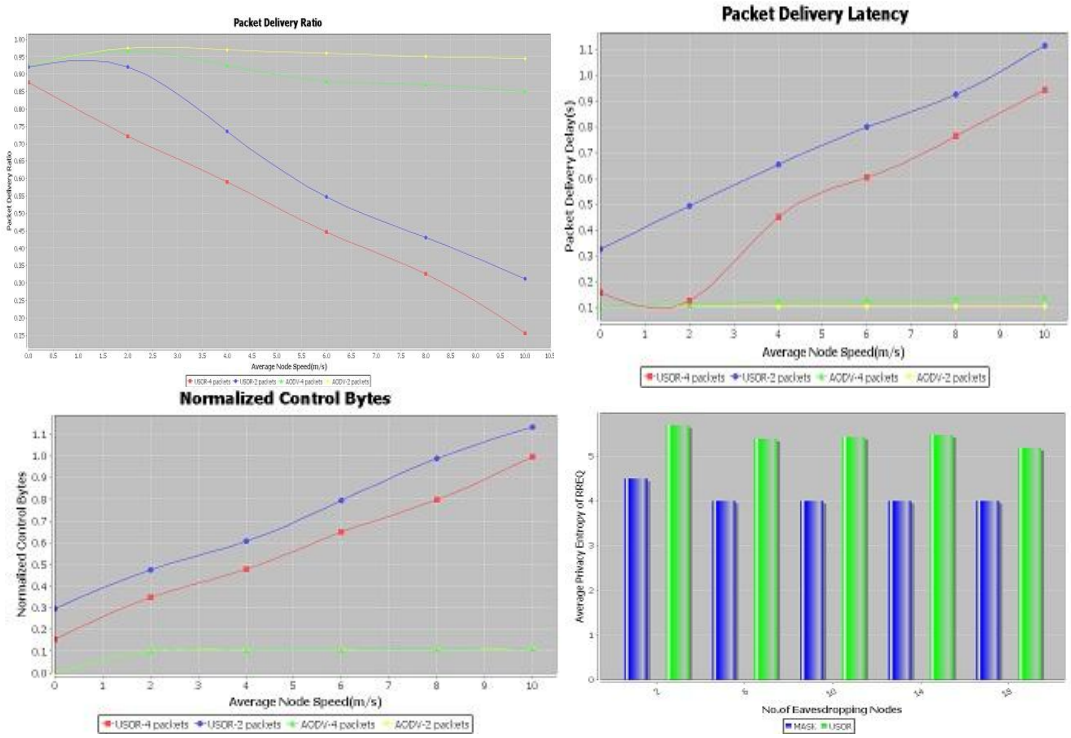
The broadcast key has been established among the nodes in the network. The key generated from the public key generated for the group.This broadcast key act like a security issue where each node should get authenticated before it enters into the network for communication.The BK will be shared among the neighbors in the zone.

2.4 Attacker Model

For the collusion attacks, USOR still offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by USOR.For preventing the Sybil attacks, the centralized key server generates group signature signing keys and ID-based keys for network nodes. Thus, it is impossible for the adversary to obtain other valid identities except the compromised ones.

2.5 Performance Evaluation

The sender computes the anonymity of RREQ packets. The sender anonymity is the obtained by calculating entropy of probability distribution of possible sender of RREQ packets.The performance has been rated by comparing the results from MASK. This results show that the error rate has been reduced.This system not only achieves anonymity, unobservability, unlinkability but also prevents from Sybil attack and collusion attack.



III. Conclusions

The USOR offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by USOR. In the padded USOR, all packets including RREQ, RREP packets and other control packets are padded to 128 bytes. Due to the packet padding, performance of the padded USOR is obviously downgraded, but the padded USOR still achieves satisfactory performance: more than 85% delivery success and about 250ms delivery latency. And also it not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. Finally, achieves stronger privacy protection than existing schemes like MASK.

References

[1] Karim El Defrawy, Member, and Gene Tsudik, Senior Member"Privacy-preserving location-based on-demand routing in MANETs," IEEE J. Sel. Areas Column., vol. 29, no. 10, pp. 1926–1934, 2011.
[2] Andreas Pfitzmann, TU Dresden and Marit Hansen, ULD Kiel "Anonymity, Unlinkability, Undetectability, Unobservability,Pseudonymity, and Identity Management –A Consolidated Proposal for Terminology"Version v0.31 Feb. 15, 2008.
[3] Jiejun Kong, Xiaoyan Hong" ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks" June 1–3, 2003.
[4] Karim El Defrawy and Gene TsudiK"ALARM: Anonymous Location-Aided Routing in Suspicious MANETs"March 2007.
[5] Reshmi Maulik and Nabendu Chaki "A Study on Wormhole Attacks in MANET " ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
[6] Nadher MohammedAhmed AI-Safwani"The Effect of Eavesdropping and Wormhole Attacks on Mobile Adhoc Networks"2009.
[7] Tanu Preet Singh, Shivani Dua and Vikrant Das" Energy-Efficient Routing Protocols In Mobile Ad-Hoc Networks" Volume 2, Issue 1, January 2012.
[8] Kortuem.G., Schneider. J., Preuitt.D, Thompson .T.G.C, F'ickas.S. Segall.Z. "When Peer toPeer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks", 1st International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001)
[9] Mangrulkar.R.S, Dr. Mohammad Atique, "Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network" (2010)
[10] Marc Branchaud, Scott Flinn,"x Trust: A Scalable Trust Management Infrastructure"
[11] Menaka Pushpa.A M.E., "Trust Based Secure Routing in AODV Routing Protocol" (2009)
[12] Sridhar, S., Baskaran, R.: Conviction Scheme for Classifying Misbehaving Nodes in Mobile Ad Hoc Networks in the proceedings of CCSIT 2012 published by Springer (LNICST) 2012
[13] "TAODV: A Trusted AODV Routing protocol for Mobile ad hoc networks" (2009)