International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

# An Unobservable Secure Routing Protocol with Wormhole Attack Prevention for Mobile Ad-Hoc Network

Vaishali Patil[Ȧ*], Priyanka Fulare[Ȧ] and Nitesh Ghodichor[Ḃ]

[Ȧ]GHRCETW, Nagpur India, [Ḃ]PCE,Nagpur India

Accepted 25 May 2014, Available online 01 June2014, **Vol.4, No.3 (June 2014)**

***Abstract***

*Privacy preserving routing is crucial in Mobile ad-hoc network for this require stronger privacy protection. An unobservable secure routing protocol with wormhole attack prevention provides anonymity, content unobservability & wormhole attack prevention in Mobile Ad-hoc Network. Unobservable secure routing protocol is based on group signature & public key encryption with multipath RREQ and their timestamp. USOR detect suspicious node in the network, trying to become isolate all suspicious node or any suspicious route, will not consider for transmission & traffic is transmitted via another shortest path.*

***Keywords:*** *Security, anonymity, routing, wormhole attack, unobservability*.

## 1. Introduction

Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. USOR achieves content unobservability by employing anonymous key establishment based on group signature. The unobservable routing protocol is executed in two phases. 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. In USOR both control packets and data packets look random and indistinguishable from dummy packets for outside world. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. A node can establish a key with each of its neighbors, and then uses such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for it by trial decryption. MANET, due to the nature of wireless transmission, has more security issues compared to wired environments. Tunneling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process.

To achieve unobservability, a routing scheme should provide unobservability for content and traffic pattern. Hence we define refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. USOR is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern unobservability. It can be used with appropriate traffic padding schemes to achieve truly communication unobservability.

## 2. Related Work

USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks 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 that achieves 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 the unobservable routing protocol is then executed in two phases. 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. USOR is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern unobservability. And it can be used with appropriate traffic padding schemes to achieve truly communication unobservability (Zhiguo Wan, Kui Ren 2012).

Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation, create many possible routs when sending route request (RREQ) from source to destination and use those routes as reference to each other, in order to find malicious node with suspicious behavior within the network. This methods works in three steps, which are routes

*Corresponding author **Vaishali Patil** is a ME WCC Student; **Priyanka Fulare** and **Nitesh Ghodichor** are working as Asst Prof.

redundancy, route aggregation and calculating round trip time (RTT) of all listed routes, route redundancy is source sends RREQ using every possible way to destination. All the routs that connect source & destination are listed together with the no. of hops from every route. Some routes gathered in the same relay point before destination is aggregated, so all nodes that join the network can be listed and the behavior of malicious nodes it can be detected. The RTT & the no. of hopes of all listed routes are compared in order to suspicious route (Soo-Young Shin 2012).

Improved AODV Routing Protocol to cope with high overhead in high mobility MANETs, AODV protocol minimizing its control messages overhead. Enhancements include developing two improved versions of AODV protocol. These two versions use Global Positioning System (GPS) to limit the routing discovery control messages. The first version (AODV-LAR) is a variation of the Location Aided Routing (LAR) protocol. The second version (AODV Line) limits nodes participating in route discovery between source and destination based on their distance from the line connecting source and destination. The delivery ratio in the proposed protocols is comparable to the delivery ratio in the original AODV (Mikki, Kangbin yim 2012).

ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. The design of ANODR is based on “broadcast with trapdoor information”, a novel network security concept which includes features of two existing network and security mechanisms, namely “broadcast” and “trapdoor information” For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; Based on onion routing for route discovery, ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability, but unobservability of routing messages is not considered in its design. For location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters (J. Kong and X. Hong 2003).

## 3. Proposed Scheme

An efficient unobservable secure routing scheme USOR provide privacy protection by employing anonymous key management process. In this protocol both control packets & data packets are look random and indistinguishable from dummy packets for outside world. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. A node can establish a key with each of its neighbors, and then uses such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for it by trial decryption. USOR comprises two phases: Anonymous trust establishment & Unobservable route discovery.

*Anonymous trust establishment:* Nodes in the networks are communicates with each other within its radio range. Nodes construct the session keys with its neighboring node for packet transmission.

*Unobservable route discovery:* 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. Source sends route request messages flood throughout the network , while the route reply message are sent backward to the source node only.

USOR provides privacy protection in terms of following parameters

*Anonymity by group signature:* The sender, the receiver and intermediate nodes are not identifiable within the whole network, it can be verified without disclosing one’s identity. Group signature is used to establish session keys between neighboring nodes, so that they can authenticate each other anonymously. And subsequent routing discovery procedure is built on top of these session keys. Hence it is easy to see that USOR fulfills the anonymity requirement under both passive and active attacks, as long as the group signature is secure

*Maintaining Unlinkability:* The linkage between the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. The nonce is only used once and never reused, and so are the pseudonyms. Except the random nonce and the pseudonym, the remaining part of the message, including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key.

*Content Unobservability:* In USOR, RREQ, RREP and data packets are indistinguishable from dummy packets to a global outside adversary. a node and its next-hop node or previous-hop node on route establish a session key anonymously, hence no one is able to know real identities of its next-hop node or previous-hop node. Even the source and the destination node do not know real identities of the intermediate nodes on route. As a result, USOR offers content unobservability.

*Wormhole Attack Prevention:* In wormhole attack adversary record information at an origin point, tunnel it to destination point more than one hop away and retransmit the information in the neighborhood of destination. Since a wormhole attack can be launched without compromising any node or the integrity and authenticity of communication.

## 4. Simulation

USOR requires a signature generation and two point multiplication in the first phase. In route discovery process, each node except the source node & destination node needs one ID-based decryption, while the source node & destination node have to do two ID-based encryption/decryption & two pint multiplications. We consider ad-hoc network consisting *n* nodes. A node can communicate with others node and these node are called its neighbor, nodes has to communicate via multiple path and each node has at least one neighbor a key server generate a group public key which is publically known by everyone and it also generate a private group signature key which means a signature does not reveal the signer’s identity but everyone can verify its validity. By verifying authenticity of each node data is transmitted from source node to the destination node this process is unobservable route discovery for successful data transmission. USOR Simulation is in NS2.

The USOR result is compared with AODV protocol, as USOR is routing protocol with privacy protection. AODV is only routing protocol, security is not consider while routing. Thus the throughput of network is more in USOR as compared to AODV protocol. Similarly energy required for successful data transmission is required more in AODV protocol, it reduces for USOR both the results are as shown in Fig 1. and Fig. 2.

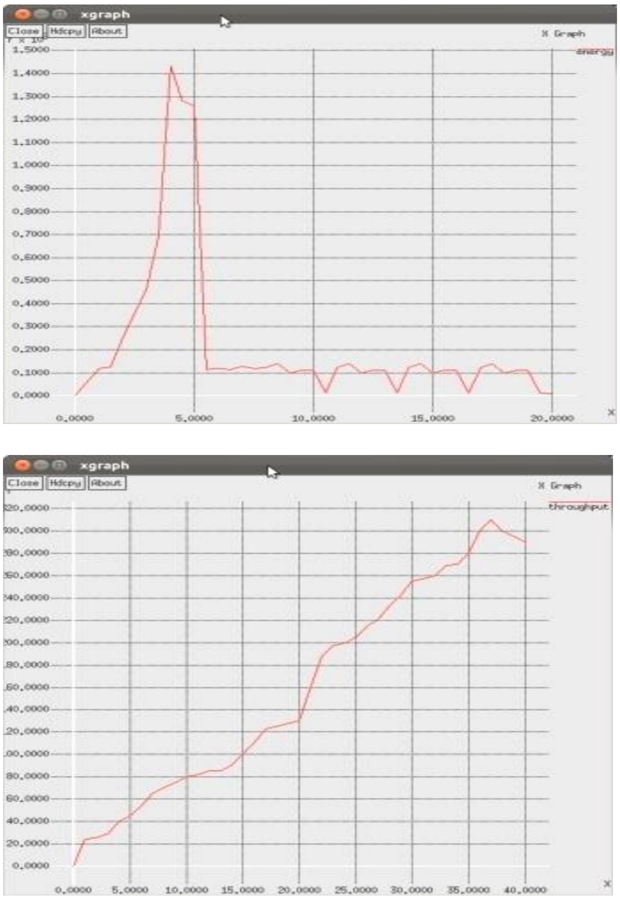
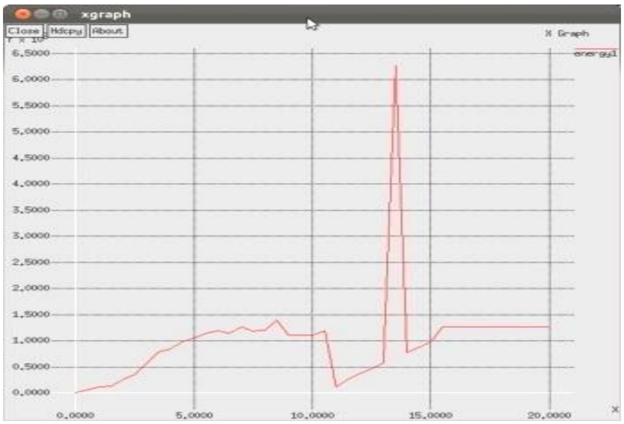


**Fig.1** Energy Consumption & Throughput of system for AODV



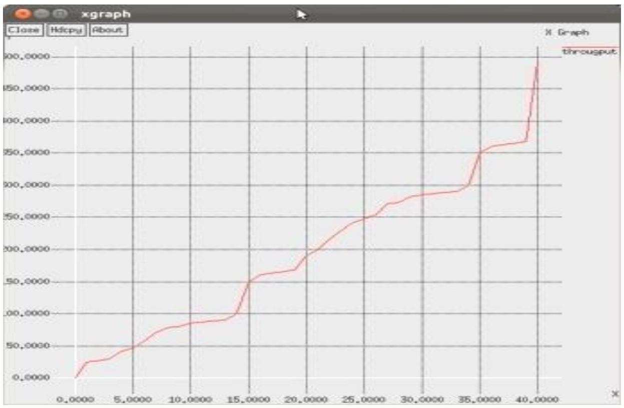


**Fig.2** Energy Consumption & Throughput of system for USOR

## Conclusions

1) Every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment.
2) USOR is based on Topology Formation & Anonymous Key establishment.
3) Privacy provides in terms of Anonymity, Unlikability and Content Unobesrvability & Wormhole attack prevention.
4) USOR performance compared with AODV Protocol.

## References

Zhiguo Wan, Kui Ren, and Ming Gu,( 2012), USOR An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks, *IEEE transactions on wireless communications*, VOL. 11, NO. 5.

Soo-Young Shin, Eddy Hartono Halim, (2012), Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation, *IEEE ICTC* 978-1-4673-4828-7/12, pp. 781-786

Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap,( 2012), Detection of wormhole attack using Hop-Count and Time delay Analysis, *International Journal of Scientific and Research Publications*, Volume 2, Issue 4.

P. Thamizharasi, D.Vinoth, (2013) Unobservable Privacy-Preserving Routing In MANET, *International Journal of Emerging Science and Engineering (IJESE)* ISSN: 2319–6378, Volume-2, Issue-3.

Mohammad Ayash, Mohammad Mikki,Kangbin yim,( 2012), Improved AODV Routing Protocol to cope with high overhead in high mobility MANETs, *ICIMISUC IEEE.*

J. Kong and X. Hong, (2003), ANODR aonymous on demand routing with untraceable routes for mobile ad-hoc networks, *ACM MOBIHOC*, pp. 291–302.

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

S. Seys and B. Preneel,(2006), ARM anonymous routing protocol for mobile ad hoc networks, *IEEE International Conference on Advanced Information Networking and Applications,* pp 133-137.

L. Song, L. Korba, and G. Yee, (2005), AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc network , *ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 33– 42.

Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, (2009), ARMR anonymous routing protocol with multiple routes for communications in mobile ad hoc networks, *Ad Hoc Networks*, vol. 7, no. 8, pp. 1536– 1550.

A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, (2007), SDAR a secure distributed anonymous routing protocol for wireless and mobile ad-hoc networks, *IEEE LCN*, pp. 618–624.

D. Sy, R. Chen, and L. Bao, (2006), ODAR on-demand anonymous routing in ad hoc networks, *IEEE Conference on Mobile Ad-hoc and Sensor Systems*.