Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Approach to Avoid Wormhole Attack

Y. Ramamohan
Vignan's Lara Institute of Tech. &Science
CSE Department

Y. Srinivasa Rao
Vignan's Lara Institute of Tech. &Science
Assistant Professor, CSE Department

Abstract: ***Now a day attacker can obtain information like sequence number and packet type etc. our main aim is to guard all parts of a packet's content, and it is self-governing of solutions on traffic pattern un-observability.***

In this project, we define solid secrecy requirements regarding secrecy-maintain routing in MANET. We propose an unobservable secure routing scheme USOR to offer complete unlink ability and content un-observability. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route outcome. Protection analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers.

Key word: Security, MANET, Routing, ID based encryption

I. INTRODUCTION

MANET is a network, which is independent network. Due to figureless property, network may be affected by attackers. To avoid security problem there are so many researchers invented many security methods like encryption methods. To improve security here we are using popular two methods, one is RSA algorithm and Sha-1 algorithm.

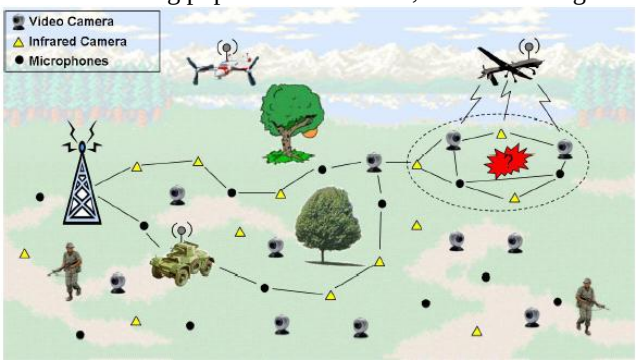


Fig.1 MANET application

In this project we suggested un-observability by providing protection on request and reply. Wormhole attack is a serious attack that may happen in ad-hoc network in which one malicious node act as a point which collect or record all the packets and tunnel these packets to another point in the network.

II. RELATED WORK

In this paper [1], author focus on a particular class of flow correlation attacks, traffic analysis attack, by which an adversary attempts to analyze the network traffic and correlate the traffic of a flow over an input link at a mix with that over an output link of the same mix.

Analyzing of mix networks was done in terms of their effectiveness in providing anonymity and quality-of-service and it shows that it can achieve a guaranteed low detection rate while maintaining high throughput for normal payload traffic but unlinkability alone is not enough in hostile environments like battlefields as important information like packet type are still available to hackers. Then a passive attacker can mount traffic analysis based on type of packet.

In this paper [2], author proposes a novel anonymous on-demand routing protocol, named MASK, to enable anonymous communications thereby thwarting possible traffic analysis hackers. Based on a new cryptographic concept called pairing, he first proposes an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities.

A pairing based anonymous on-demand routing protocol MASK is which provides strong sender and receiver namelessness, the relationship anonymity between receivers and senders, the un-locatability of mobile nodes and the un-traceability of packet flows under a rather strong adversarial model but the routing information is not authenticated in the current design of MASK.

In this paper [3], author proposes a fully self-organized public-key management system that allows users to generate their public and private key pairs, to publish certificates and to perform authentication regardless of the network partitions and without any centralized services. Moreover, this approach does not require any trusted potency, not even in the system initialization phase.

Self-organized public-key management scheme is proposed that does not rely on any trusted authority or defined server, not even in the initialization stage. Author showed that with a simple local repository construction algorithm and a small communication overhead, this system achieves high performance on a wide range of certificate graphs but it requires users' conscious involvement only when their public/private key pairs are created and for issuing and revoking certificates.

In this paper [4], author develops an untraceable routes or packet flows in an on-demand routing environment. This aim is very different from other related routing security problems such as resistance to route disruption or prevention of denial-of-service attacks.

An anonymous on-demand routing protocol ANODR for mobile ad hoc networks deployed in hostile environments. It demonstrates that untraceable data forwarding without encrypted routing header can be efficiently realized but main disadvantage of this mechanism is that all nodes receiving the RREQ message must try to decrypt the global trapdoor to find out whether it is the intended receiver, ensuing in considerable overhead.

[5] In this paper, author proposes an Anonymous Secure Routing protocol that can provide additional properties on namelessness, i.e. Identity Anonymity and Strong Location Privacy, at the same time ensure the security of discovered routes against various passive and active attacks.

The Anonymous Secure Routing protocol is proposed which provides more anonymity and security to the mobile ad-hoc networks which was a drawback in previous protocols but in the cases of route changes or link failures some problems will arise in this protocol.

III. EXISTING SYSTEM

A number of secure routing outline have been brought forward MASK is based on a special type of public key crypto system and the pairing-based cryptosystems are to achieve anonymous communication in MANET

3.1 Disadvantages:

Existing schemes fail to protect all content of packets from hackers, so that the attacker can obtain data like packet type and sequence numbers etc. These details can be used to relate two packets, which break unlink ability and may lead to source trace back attacks.

Another disadvantage of earlier outlines is that they rely deeply on public key cryptography and thus incur a very high computation overhead.

VI. PROPOSED SYSTEM

In this project, we introduced an efficient privacy maintain routing protocol USOR that achieves content un-observability by employing anonymous key establishment based on group signature.

There are two types of unobervability in MANET. Content unobsevability and traffic pattern unobervability. Content Un-observability means no useful information can be extracted from any message content. Here using content unobsevability to prevent wormhole attack. The unobservable routing protocol uses group signature for key establishment. Using this key establishment it provides the content unobsevability. The private key is generated by a key management scheme like key server and the group id is generated by leader node.

4.1 Advantage:

This project is implementing high security data transfer so we can avoid hacking unlike data security, it providing the basic packet security also.

V. UN-OBSERVABILITY IMPLEMENTATION

Algorithm for Enhanced USOR:

1. Initialize the nodes as follows
    a. Leader node: (it can share the key at initial time)
    b. Normal node: (normal mobile node)
2. Leader node initially sends the Group ID key to all then mobile node
3. If normal node received that ID then stores into memory
4. If node having GID
    a. It can access the request
5. If not
    a. Can't access the request
6. If node (i) wants to communicate with another node
    a. Node i generates the hash code(by sha-1)
    b. Encrypting (by RSA) that code with private key of node i
    c. And sends to dest… node
7. destination node can verify that encrypted message by using the public key and as well as group ID
    a. if match
        a.i. node j sending own code to source node i
    b. if not match
        b.i. ignore

8. if match code of node j
    a. transfer the data
9. if not match
    a. ignore

VI. PROJECT DESCRIPTION

In this project, we define solid privacy requirements regarding privacy-maintain routing in MANET. We propose an unobservable secure routing scheme USOR to offer complete unlink ability and content un-observability for all types of packets. USOR is efficient as it uses a novel arrangement of group signature and ID-based encryption for route discovery. The simulation results show that USOR not only has satisfactory performance compared to AODV, but also achieves stronger confidentiality defense than existing schemes like MASK

6.1 Modules:

- Basic routing module
- Include hacking in basic routing module
- Protection against hacking

6.1.1 Basic Routing Module:

If the source has no route to the destination, then source initiates the route discovery in an on-demand fashion

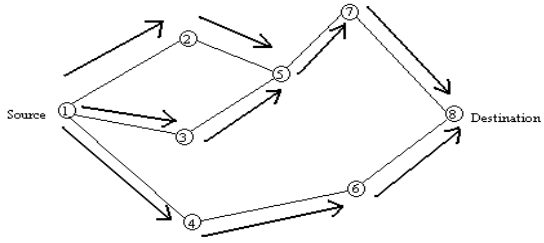
Past generating RREQ, node looks up its have possession of neighbor table to find if it has any closer neighbor node toward the destination vehicle.

If a nearer neighbor node is available, the RREQ packet is forwarded to that vehicle.

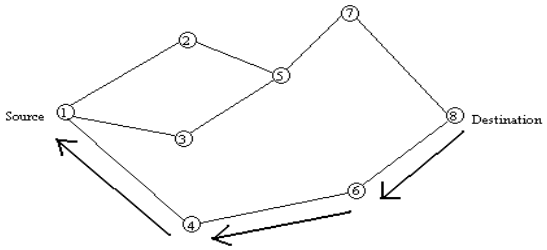
If no earlier neighbor node is the RREQ packet is flooded to all neighbor nodes.

A destination node replies to a received RREQ packet with a route reply (RREP) packet in only the following three cases:

1) If the RREQ packet is the first to be acknowledged from this source vehicle



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

2) If the RREQ packet contains a upper source sequence number than the RREQ packet previously responded to by the destination vehicle
3) If the RREQ packet has the same source sequence number as the RREQ packet previously responded to by the destination node, but the new packet indicates that a better quality route is available.

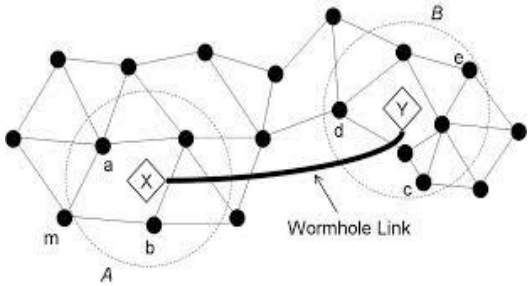
6.1.2 Include hacking in basic routing module:

In this module we are including the hacking node with our network so the attacking node creates problem.

And now we are going to analyze our current network status with some problem and able to solve it.

Wormhole attack:-

Wormhole attack is a serious attack that may happen in adhoc network in which one malicious node act as a point which collect or record all the packets and tunnel these packets to another point in the network.

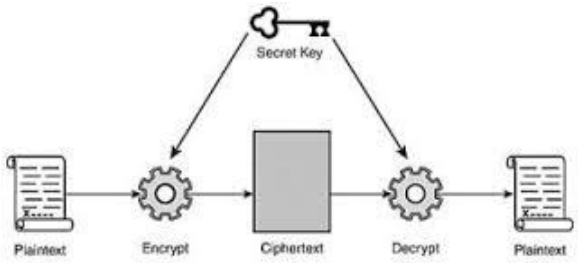


Here X and Y create a wormhole link and it act as the smallest path between the two nodes and send the data using this particular link only. Due to this fake route all the data select this as the shortest path and this may cause serious threat to the network. This is a passive attack, means it never change the functionality of the network but it may cause packet drop or packet lose. So it is very difficult to detect. This normally occurs due to multiple adversaries in a network.

6.1.3 Protection against hacking:

In this module, we are implementing USOR by protecting all information about that particular packet.

In this module the packet is identified by authorized user's only, other node can't identify information about that packet.



VII. ANALYSIS

Network performance refers to the service quality of a communications product as seen by the customer. There are many different ways to measure the performance of a system, as each system/network is dissimilar in nature and design.

1) Packet delivery function.

PDF is the term used to measure the network performance. PDF defines the how much packet delivered correctly over total number of packet sent

2) Overhead.

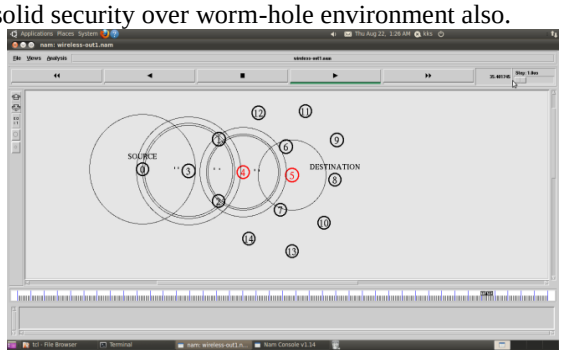
Overhead is the one important concept to analyze network performance. Overhead is defined as number of routing and control packet is requiring transferring the data.

VIII. RESULT

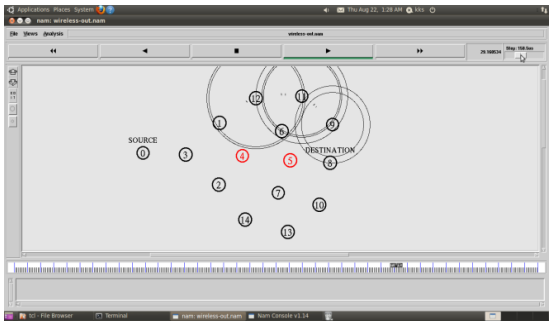
In our project, we analyzed different network environment with main network parameters such as packet delivery radio and overhead.

Result shown bellow is packet delivery function. In that graph, there are the three environments (without malicious environment, with malicious environment and USOR environment) shown.

In previous work the researcher tested only black hole attack in our work we tested with worm-hole attack also. From our result USOR providing solid security over worm-hole environment also.



Wormhole attack in MANET

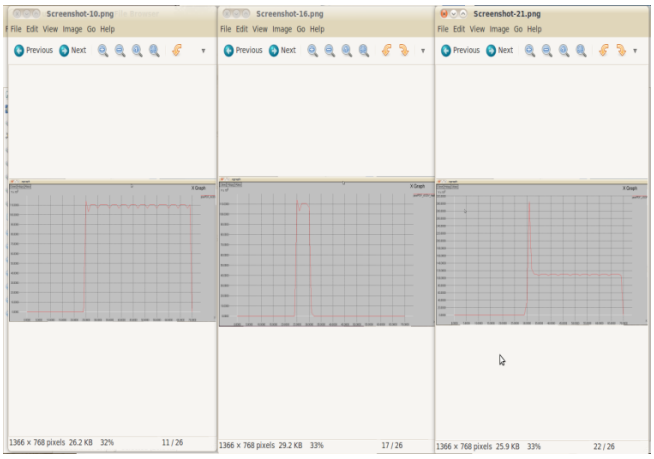


Prevention against wormhole attack by USOR

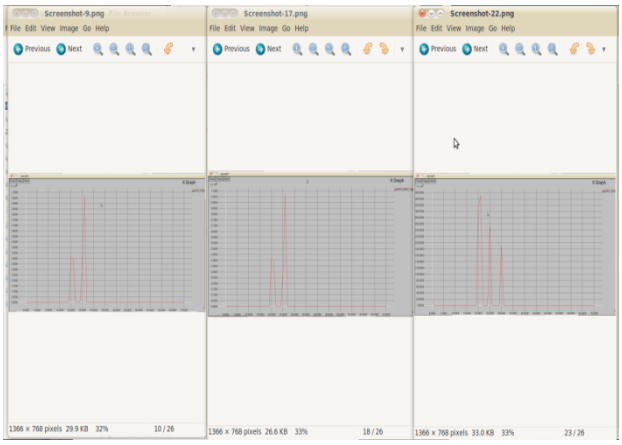
Table1: performance comparison

Protocol	*PDF(%)*	*OH(pkt)*	*Delay(ms)*
AODV	89.926	316	37
Mali	8	316	400
USOR	82	183	38

From our result, we will grasp we have a tendency to improved our network performance.
From our result, we can know we improved our network performance



The graph shown bellow is overhead graph, from this result we can know USOR has more overhead than normal AODV. USOR performance is better than normal AODV even overhead is more; the reason is security of USOR is very high so overhead is ignorable in this case.



OH Comparison b/w AODV, Mali_AODV and USOR

After preventing the wormhole attack the data packets select another route to destination.

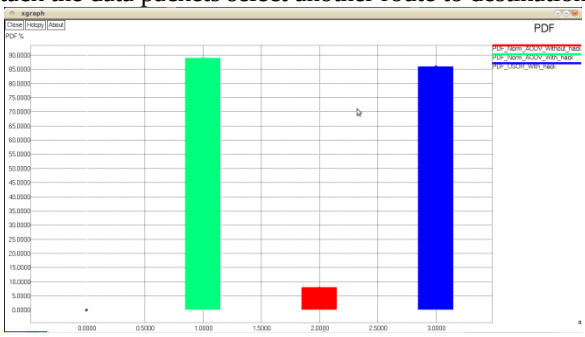


Fig7: Comparison of basic AODV and Proposed model in malicious environment

The graph shows the packet delivery performance of the modified protocol is very high in wormhole environment.

IX. CONCLUSION

In this paper, we suggested an unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks. The conception of USOR offers solid privacy protection complete unlinkability and content unobservability for ad hoc networks. The protection analysis demonstrates that USOR not only provides strong retreat security, it is also more resistant against attacks due to node compromise.

REFERENCE

[1] *"On Flow Correlation Attacks and Countermeasures in Mix Networks"* Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao.

[2] *"Anonymous Communications in Mobile Ad Hoc Networks"* Yanchao Zhang, Wei Liu and Wenjing Lou.

[3] *"Self-Organized Public-Key Management for Mobile Ad Hoc Networks"* Srdjan Capkun, Levente Butty´ n and Jean-Pierre Hubaux.

[4] *"ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks"* Jiejun Kong, Xiaoyan Hong.

[5] *"Anonymous Secure Routing in Mobile Ad-Hoc Networks"* Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng.

[6] *"ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks"* Stefaan Seys and Bart Preneel.

[7] *"SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks"* Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba.

[8] *"ALARM: Anonymous Location-Aided Routing in Suspicious MANETs"* Karim El Defrawy and Gene Tsudik.

[9] *"Identity-Based Encryption from the Weil Pairing"* Dan Boneh, Matthew Franklin.

[10] *"SybilGuard: Defending Against Sybil Attacks via Social Networks"* Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman.

