Secure Routing In Mobile Adhoc Networks Using USOR Resistant Against DOS Attack

Mahesh Kumar. M[1], Saravanan. S[2],

M.E-Student[1], Assistant Professor[2],

Department of CSE[1], Department of IT[2],

Srinivasan Engineering College, Perambalur, TN, India

Abstract—Mobile ad hoc networks often support sensitive applications. These applications may require that users' identity, location, and correspondents be kept secret. This is a challenge in a MANET because of the cooperative nature of the network and broadcast nature of the communication. A number of anonymous routing schemes have been proposed for ad hoc networks to provide better support for privacy protection but bring significant computation overhead. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. The wormhole attacks cannot be prevented in USOR mechanism. The proposed system aimed at developing unobservable routing scheme resistant against DoS attacks such as Gray hole/Black whole attacks to protect network-layer reactive protocols. It discovers malicious nodes during route discovery process when they mitigate fabricated routing information to attract the source node to send data through malformed packet. Security analysis demonstrates that USOR can well protect user privacy against internal and external attackers. The simulation results show that it achieves stronger privacy protection than existing schemes.

Index Terms— anonymous key establishment, group signature, malicious node, privacy protection.

I. INTRODUCTION

A MANET is a decentralized networkconsisting of set of mobile nodes communicates with each other in shared wireless medium. Each node has limited communication range in the network and acts as a router to forward packets to another node. Privacy concerns are increasing in the Internet and wireless networks due to the mounting intrusions and attacks. Anonymity that hides the identities of various components or parts of a network communication is one of the countermeasures. Strong anonymity in network communication prevents address spoofing, route forgery, and certain denial of service (DoS) attacks by concealing the true identity of the traffic. 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. MANETs are vulnerable to various types of DoS attacks on network layer. In specific Gray hole and Black hole attacks malicious nodes deliberately disrupt data transmission in the network by sending incorrect routing information. These attacks disturb route discovery process and degrade network's performance. Thus it is a challenge to keep the communication route free from such attackers.

This paper proposes an efficient protocol to protect the network-layer reactive protocols from DoS attack. The proposed malicious node resistant scheme detects the malicious node sending false routing information. The routing packets are used not only to pass routing information but also to pass information about malicious nodes and detect the malicious node during route discovery process when they evade fabricated routing information to attract the source node to send data through itself. The contribution of this paper includes

(i) Establishes safe and secure communication,

(ii) An unobservable secure routing scheme employing anonymous key establishment based on group signature.

(iii) It provides strong privacy preserving routing for ad hoc networks and also resistant against attacks due to node compromise.

II. RELATED WORK

The wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. The existing security solutions for wired networks cannot be applied directly in wireless MANETs. Applications that make use of ad hoc routing have heterogeneous security requirements.

Authentication, *message integrity*, and *non-repudiation* to an ad hoc environment Ease of Use are part of a minimal security policy. Apart from these, there are several other security issue such as *black hole attacks, denial of service*, and *information disclosure*.

The Protocol for Anonymous Routing (PAR), based on public key cryptography, to provide absolute anonymity. With this we achieve complete sender and receiver anonymity. Also, the sender and the receiver cannot be linked to each other even if all the nodes in the established path collaborate. However, with absolute anonymity defending against denial-of-service attacks by compromised nodes becomes very difficult. Hence, to detect and defend against these attacks, we present PAR-Enhanced, a variation of the above protocol, which only provides quasi-absolute anonymity .We consider the anonymity properties provided to an individual node against two distinct types of attackers:

A *local eavesdropper* is an attacker who is also the neighbor of the sender/receiver and hence, can observe all (and only) communication to and from the sender/receiver .*Collaborating nodes* are *other* nodes that can pool their information.

LE-S denotes *local eavesdropper of the sender* and LE-R denotes *local eavesdropper of the receiver*. Also, it should be noted that consists of collaborating nodes and does not consist of local eavesdroppers. Of course, against an attacker who is comprised of both of the attackers described above, the protocol yields degrees of sender and receiver anonymity that are the minimum provided against the attackers present

Ad hoc wireless networks assume that no pre-deployed infrastructure is available for routing packets end-to-end in a network, and instead rely on intermediary peers. Securing ad hoc routing presents challenges because each user brings to the network their own mobile unit, without the centralized policy or control of a traditional network. Many ad hoc routing protocols such as Dynamic Source Routing (DSR), Ad Hoc On Demand Distance Vector (AODV), Zone Routing Protocol (ZRP), and Location Aided Routing (LAR) have been proposed previously, but none of the proposals have defined security requirements, and all inherently trust all participants .All proposed protocols have security vulnerabilities and exposures that easily allow for routing attacks. These vulnerabilities are common to many protocols. The fundamental differences between ad hoc networks and standard IP networks necessitate the development of new security services. In particular, the measures proposed for IPSec help only in end-to-end authentication and security between two network entities that already have routing between them; IPSec does not secure the routing protocol. While mechanisms similar to those used in IPSec can be adapted to secure the routing, IPSec alone does not suffice .This point has been recognized, and others have started to examine security problems in ad hoc networks. A solution that uses threshold cryptography as a mechanism for providing security to the network is presented in . A method that ensures equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates is presented . An effort to secure an existing ad hoc routing protocol has also recently been made available .Apart from the above protocols, which try to deal with minimal security requirements like Authentication, message integrity, and non-repudiation, several other protocols were presented to deal with specific security issues encountered in MANETs. presents the resurrecting duckling security policy model, which describes secure transient association of a device with multiple serialized owners. presents a solution to prevent black hole attacks, presents strategies for intrusion detection.

III. TECHNIQUES

Ad hoc network routing security

In this section, we define taxonomy of types of attackers and discuss specific attacks against ad hoc network routing. This approach allows us to categorize the security of an ad hoc network routing protocol based on the strongest attacker it withstands.

Attacker model

We consider two main attacker classes, *passive* and *active*. The passive attacker does not send messages; it only eavesdrops on the network. Passive attackers are mainly threats against the privacy or anonymity of communication, rather than against the functioning of the network or its routing protocol, and thus we do not discuss them further here. An active attacker injects packets into the network and Generally also eavesdrops. We characterize the attacker based on the number of nodes it owns in the network, and based on the number of those that are good nodes it has compromised. We assume that the attacker owns all the cryptographic key information of compromised nodes and distributes it among all its nodes.

General attacks on ad hoc network routing protocols

Attacks on ad hoc network routing protocols generally fall into one of two categories: *routing disruption* attacks and *resource consumption* attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory(storage) or computation power. From an application-layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack. An example of a routing disruption attack is for an attacker to send forged routing packets to create a *routing loop*, causing packets to traverse nodes in a cycle without reaching their destinations, consuming energy and available bandwidth. An attacker may similarly create a routing *black hole*, in which all packets are dropped: by sending forged routing packets, the attacker could cause all packets for some destination to be routed to itself and could then discard them, or the attacker could cause the route at all nodes in an area of the network to point “into” that area when in fact the destination is outside the area. As a special case of a black hole, an attacker could create a *gray hole*, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets. An attacker may also attempt to cause a node to use *detours* (suboptimal routes) or may attempt to *partition* the network by injecting forged routing packets to prevent one set of nodes from reaching another.

AN UNOBSERVABLE ROUTING SCHEME

In this section we present an efficient unobservable routing scheme USOR for ad hoc networks. 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.

The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery. The unobservable routing scheme USOR aims to offer the following privacy properties.

1) Anonymity: the senders, receivers, and intermediate
Nodes are not identifiable within the whole network, the
Largest anonymity set.

2) Unlinkability: the linkage between any two or more
IOIs from the senders, the receivers, the intermediate
nodes, and the messages is protected from outsiders.
Note linkage between any two messages, e.g., whether
they are from the same source node, are also protected
.

3) Unobservability: any meaningful packet in the routing
scheme is indistinguishable from other packets to an
outside attacker. Not only the content of the packet but
also the packet header like packet type are protected
from eavesdroppers. And any node involved in route
discovery or packet forwarding, including the source
node, destination node, and any intermediate node, is
not aware of the identity of other involved nodes (also
including the source node, the destination node, or any other intermediate nodes).

Notation and Definitions

Public and Private Keys*:* The presence of a Public Key Infrastructure. We denote the private and public keys of a node *i* as *Ei* and *Di*. We denote the E(M, k) and D (M, k) to denote the encryption and decryption of message M with key k.

Route Requests

Whenever a node S wishes to communicate with a node D, it initiates the route discovery process. Route discovery allows any node in the ad hoc network to dynamically discover a route to any other node in the ad hoc network, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other nodes. A node initiating a route discovery broadcasts a route request, which may be received by those nodes within wireless transmission range of it.

The route request has the following fields:

-FID (U*nique request identifier*, also referred to as *unique flow identifier*) is set by the source by encrypting its address (S), destination address (D) and a locally

*This time *Th* depends on the diameter of the network and could be set to the maximum Round Trip Time that could be possible in the network between any two nodes.

IAi = E(E((*i*,FID, timestamp, RP),E*i*),D*i*)maintained sequence number (SEQ) with the public key of S. This is used to detect duplicate *route requests* received at an intermediate node.

FID = E ((S, D, SEQ), Ds)

-ESA (Encrypted Source Address) is constructed by encrypting source address, hash of FID, timestamp and the Redundancy Predicate (RP) with the destination’s public key. The hash of FID and the timestamp are to prevent replay attacks.

ESA = E ((S,H(FID), timestamp, RP), DD)

EDA (Encrypted Destination Address) is constructed by encrypting destination address, hash of FID, timestamp and the Redundancy Predicate (RP) with destination public key

EDA = E ((D, H(FID), timestamp, RP), DD)

FUNCTIONAL DESIGN AND ANALYSIS

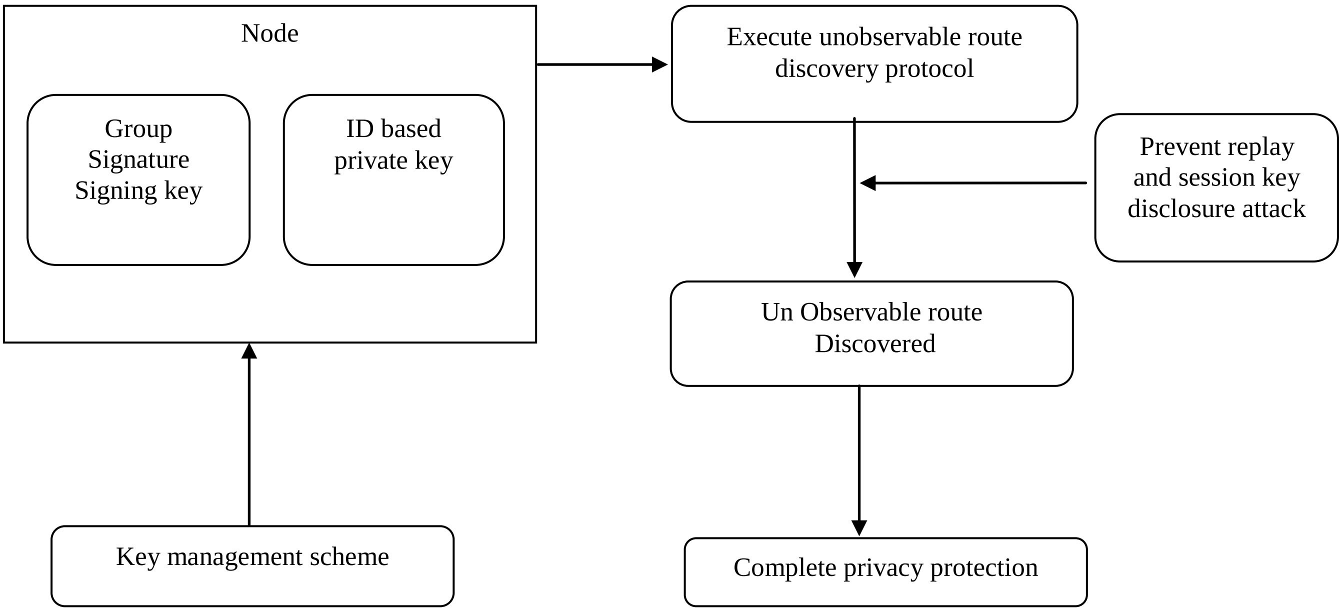
Node
Group Signature Signing key
ID based private key
Key management scheme
Execute unobservable route discovery protocol
Prevent replay and session key disclosure attack
Un Observable route Discovered
Complete privacy protection

Fig 1: Overview architecture

$$ITA = E\,(\,E((i, \mathrm{FID}, \mathrm{timestamp}, \mathrm{RP}), \mathrm{E}i\,), \mathrm{D}i\,)$$

Whenever a node *i that is not the destination* receives a non-duplicate* route request packet, it performs the following operations:

RQ1. A new entry is added to the routing flow table with FID and IPA fields set to FID and ITA values of the route request packet.

RQ2. The node checks if the route request is intended for it by decrypting the EDA with its private key *Ei* and if it is the case it proceeds to send a route reply (described below) and steps 3 and 4 are not executed.

RQ3. The timer is initiated

RQ4. Invisible address is computed for the packet and the route request is retransmitted with its ITA set to the invisible address computed.

Route Replies

The destination after receiving the route request also adds a new entry to its RFT in a similar manner as above. The destination also validates the source by decrypting ESA with E*i*.

RP1. An entry corresponding to FID is searched for in the RFT. If no entry is found, the packet is dropped and all further steps are skipped.

Then, the destination in order to establish a connection, constructs a route reply packet with the following fields:

FID is set to the FID of the route request.

ESA (Encrypted Source Address) is constructed by encrypting D (destination of route request), hash of FID, timestamp and the Redundancy Predicate (RP) with the

Only FID is considered in deciding if a route request is a duplicate or not.INA field is set only when a corresponding route reply packet is received.

$$\mathrm{FID} = \mathrm{E}((\mathrm{S}, \mathrm{D}, \mathrm{SEQ}), \mathrm{Ds}\,)$$

EDA (Encrypted Destination Address) is constructed by encrypting S (source of route request), hash of FID, timestamp, and the Redundancy Predicate (RP) with the source's public key.

$$\mathrm{EDA} = \mathrm{E}((\mathrm{D}, \mathrm{H}(\mathrm{FID}), \mathrm{timestamp}, \mathrm{RP}), \mathrm{Ds}\,)$$

ITA (Invisible Transmitter Address) is the invisible address of the node *i* transmitting the route request.

$$ITA = \mathrm{E}(\,\mathrm{E}((i, \mathrm{FID}, \mathrm{timestamp}, \mathrm{RP}), \mathrm{E}i\,), \mathrm{D}i\,)$$

IFA (Invisible Forwarder Address) is initially set to the ITA of the corresponding route request packet.

Whenever a node *i* that is not the source, receives a route reply packet, it performs the following operation

RP2. The IFA value is verified by checking for RP, its address, FID and the timestamp in D(D(IFA, D*i*), E*i*). If the verification fails, the packet is dropped and all further steps are skipped.

RP3. The INA value of the entry corresponding to FID in RFT is set to ITA of the route reply and the timer of the corresponding entry is nullified.

RP4. The INA value of the route reply packet is set to the ITA value of the entry corresponding to FID and ITA value of the route reply is set to the invisible address of *i*. The route reply is then forwarded. When the source receives the route reply, it can verify the destination address by decrypting the ESA and EDA fields in the route reply with its private key. After the verification, the source and destination can securely communicate with each other.

Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman protocol was the first public key algorithm ever invented. Diffie-Hellman can also be used for key distribution—two nodes A and B can use this to generate a secret key. First, A and B agree on a large prime, n and g, such that g is primitive mod n. These two integers do not have to be secret; they can even be common among a group of users.

Then, the protocol is as follows:

(i) A chooses a large integer *x* and sends B

X = g*x* mod n

(ii) B chooses a random large integer y and sends Alice

X = g*x* mod n

(iii) A computes k=Y*x* mod n

(iv) B computes k'=Xy mod n

Both k and k' are equal to g*x*y mod n. No one listening on the channel can compute that value, unless they can compute the discrete logarithm and recover *x* or y. So, k is secret key that A and B computed independently.

IV.EXPERIMENTAL RESULT

In this section, we analyze computation cost of USOR,

And compare it with existing schemes. We then describe the implementation and performance evaluation of our protocol. 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-based encryption/decryption and two point multiplications. MASK is not listed in the table as they do not need public key operations during the route discovery process. However, MASK does not offer sender anonymity or receiver anonymity. The USOR can achieve unobservability without too much computation cost. We implement both USOR and MASK on ns2, and evaluate their performance by comparing with AODV.

We evaluate the performance of USOR in terms of *packet delivery ratio*, *packet delivery latency*, and *normalized control bytes*. With Fig. 2 we demonstrate performance of USOR,MASK and AODV at different moving speeds for two different traffic loads. Two traffic loads are selected according to Performance of the standard AODV implementation of ns2

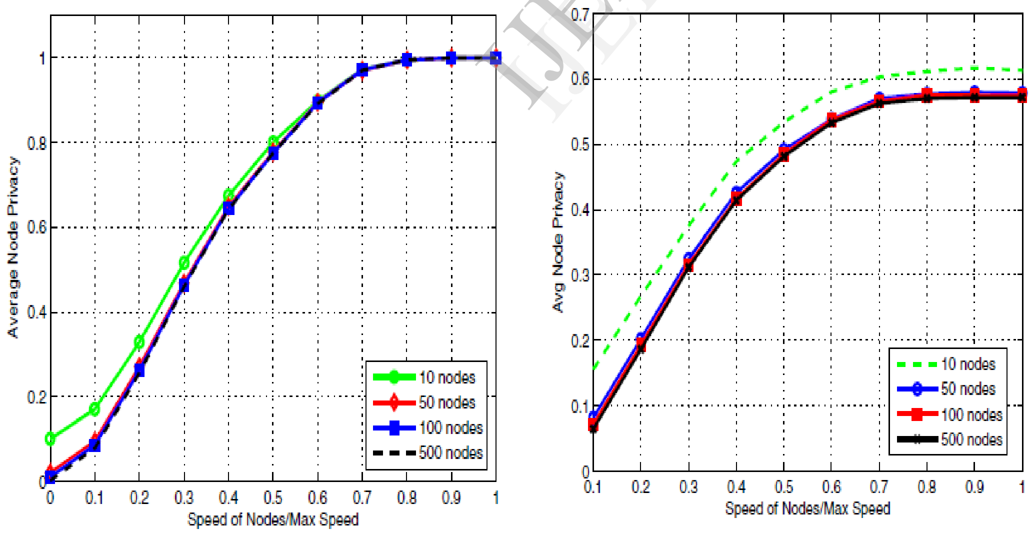

Fig 2: packet delivery ratio between AODV and MASK

V.CONCLUSION AND FUTURE WORK

The security analysis demonstrates that USOR not only provides strong privacy protection but also more resistant against attacks due to node compromise. The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information. As there is no extra control packets added in the proposed algorithm, Packet Delivery Ratio (PDR) would be improved greatly as the malicious nodes are isolated. The routing protocols mainly focused on the methods of routing, but in future a secured but QoS-aware routing protocol could be worked on.

REFERENCES

[1] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile adhoc networks," in Proc. ACM MOBIHOC'03.

[2] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile adhoc networks," in Proc. 2004 IEEEConference on Local Computer Networks.

[3] S. Seys and B. Preneel, "ARM: anonymous routing Protocol for mobile ad hoc networks," . 2006IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

[4] Y. Dong, T. W. Chim, "ARMR: anonymous routing Protocol with multiple routes for communications in Mobile ad hoc networks," Ad Hoc Networks, vol. 7, 2009.

[5] 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.

[6] Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks yih-chun hu and Adrian perrig
Carnegie Mellon University, USA-2005

[7] L. Song,L. Korba,and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc Networks," in Proc. 2005.

[8] A. Pfitzmann and M. Hansen, "Anonymity, Unobservability and pseudonymity: a consolidated Proposal for terminology," draft, July 2000.

[9] Anonymous Routing for Mobile Wireless Ad Hoc Networks Arjan Durresi and vamsi paruchuri Department of Computer Science, USA-2007.

[10] S. Capkun, L. Buttyan, and J. Hubaux, "Self organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, Jan.-Mar. 2003