SECURE ONION BASED ROUTING FOR MANETs IN ADVERSARIAL ENVIRONMENT

[1]ARCHANA.R, [2]Mrs. GRACY THERESA.W

[1]P.G SCHOLAR*, [2]ASSISTANT PROFESSOR,
[1]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,
[2]ADHIYAMAAN COLLEGE OF ENGINEERING, HOSUR, INDIA

***ABSTRACT*: Shadowy articulation is earnest for progressively the entreaty of the Mobile Ad hoc Network that have been deployed in adversary nature. A noteworthy prerequisite on the system is to give unidentifiability and unlinkability to portable hubs and their traffics. In spite of the fact that various unknown secure steering conventions have been proposed, the necessity is not completely fulfilled. The current conventions are defenceless against the assaults of fake directing parcels or denial- of- service (DoS) broadcasting, even the node identities are secured by pseudonyms. In order to satisfy the requirements and to defend the attacks a new routing protocol Authenticated Anonymous Secure Routing (AASR), have been proposed to give obscurity and network security. This protocol uses a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage and a Group signature is used to authenticate the RREQ packet one hop, to prevent intermediate node from altering the directing packet. Extensive simulations are done based on this protocol, to provide maximum throughput and minimized packet loss ratio.**

KEY WORDS: AASR, anonymous, MANETs, location privacy.

I. INTRODUCTION

MANET is defined as a self configuring less infrastructure network where mobile devices are connected without wires .Each devices in the MANET is free to move independently in any direction and in therefore change its link to any other devices frequently. They do not need have any fixed infrastructure to be configured which makes it more suitable to be used in environments that require on the fly setup. In MANET it is difficult to provide trusted and secure communications in competitor nature, such as battlefields. The competitors outside a network may infer the information about the articulating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. As a result, shadowy and trust based articulation are important for MANETs in competitor nature, In order to provide a secure communication the security is provided by authenticating the route request packet hop per hop and increases the throughput based on key encrypted onion and group signature.

II. RELATED WORK

In existing system there are many anonymous on-demand routing protocols that has been divided into two categories[1]:

- Topology-Based or Node Identity Centric
- Location-Based or Location Centric

The routing protocols are designed to work in different scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services. The existing system mainly focused on the topology-based routing rather than location-based routing, so SDAR, AnonDSR, MASK, and D-ANODR are the topology based routing protocols.

1. SECURE DISTRIBUTED ANONYMOUS ROUTING PROTOCOL

Secure Distributed Anonymous Routing Protocol [3] has been proposed to provide security, anonymity and high reliability of the established route in a hostile environment such as ad hoc wireless network by using the neighbour discovery scheme, which is used to identify the neighbours in the communication range. The major objective of this protocol is to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes.

2. ANONYMOUS DYNAMIC SOURCE ROUTING

Anonymous Dynamic Source Routing for Mobile Ad Hoc Networks have been proposed based on the analysis to provide three levels of security protection such as Security, anonymity, and scalability. This protocol uses cryptographic mechanism that is Diffie Hellmann key agreement to create a shared session key for a security communication between the source node and destination node.

3. MASK

MASK[5] is a novel anonymous on demand routing protocol, This protocol have been proposed to enable both anonymous MAC layer and network-layer communications so as to thwart adversarial, passive eavesdropping and various types of attacks by using Pairing Based Cryptography. MASK provides the anonymity of sender's relationships, receiver's relationships and sender-receiver relationships, as well as node unlocalability and untrackability and end-to-end flow untraceability. This protocol is resilient to a wide range of attacks. But MASK has comparably high routing efficiency when compared to classical AODV routing protocol while achieving the nice anonymity property. This protocol deals with passive attacks.

4. ANONYMOUS ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

Stefaan Says et.al [8] presents a mysterious on interest directing plan for MANETs where the source and the destination share a mystery key KSD and a mystery pen name. The source will incorporate this pen name the course asks for message. The destination will have a rundown of nom de plume by various sources in its memory and it confirms whether the message is focused at it or not. This alias utilized once (for a solitary course ask for message). The destination sends the answer with the same nom de plume. On the receipt of the answer message source begins to send the information alongside the onetime identifier appended with them. One time identifier shields the information from the aggressor.

5. ANONYMOUS ON DEMAND ROUTING WITH UNTRACEABLE ROUTES FOR MOBILE AD HOC NETWORKS

J. Kong et.al proposed an approach which consists of three phases. Anonymous route disclosure, Anonymous route maintenance and Anonymous route forwarding. Route disclosure phase includes route request and route reply message. It implements symmetric key agreement between two consecutive RREP forwarders and enforces destination-initiated RREP procedure. For the maintenance of the anonymous route, the routing table passages are reused upon timeout T. The evaluations of ANODR decrease when the portability of the nodes increases. And for route forwarding the trapdoor information is used.

III. OVERVIEW AND EXPLANATION

a. ONION ROUTING

It is a mechanism to provide private communications over a public network in which the sender and the receiver nodes communicate with each other anonymously by means of some intermediate nodes called onion routers. It relies on public key cryptography. The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

b. GROUP SIGNATURE

Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own particular private key, and such mark can be confirmed by different individuals in the gathering without uncovering the endorser's personality. Only the group trust authority can trace the signer's identity and revoke the group keys.

c. WORKING MECHANISM

Based on the AODV protocol the source node telecasts a RREQ packet to each node in the network. If the destination node gets the RREQ to itself, it wills response with an RREP packet back along the incoming path of the RREQ. To secure the anonymity when exchanging the route information Onion routing method and group signature is utilized. Onion routing is the mechanism in which the sender and the receiver nodes communicate with each other anonymously by means of some intermediate nodes called as onion routers it relies on public key cryptography. For Example the below figure 1 contains 6 nodes, let onion routers 4, 3, and 5 be arbitrarily selected by the onion proxy to send the data.

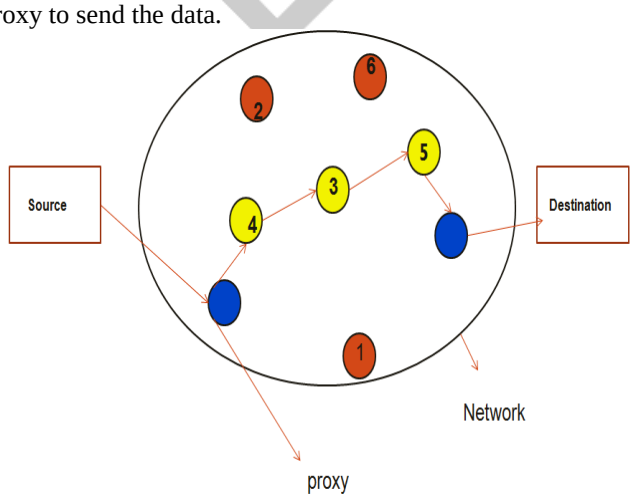

Figure 1 Onion Routing Mechanism

In the figure 1 each and every node is provided with a group public and private key based on the group signature method .The private key is unique for each and every node whereas the public key is the same for all the nodes in the group. The proxy encrypts the data with 5's public key followed by 3 and then 4.Thus an onion created in figure 2 is represented as

E4PU (3's IP address, E3PU ((5'sIP address,(E5PU(recipients IP address, data))))).

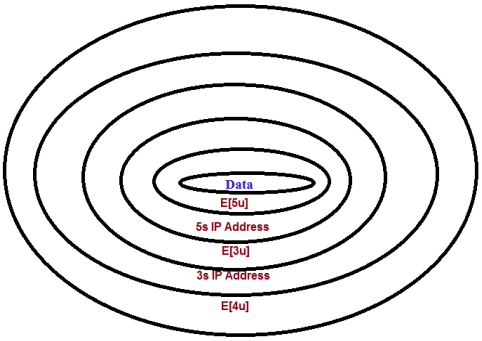

Figure 2 Key Encrypted Onion

The proxy then sends the onion to the first onion routers i.e 4. Onion router 4 peels the outer layer of the onion using its private key. It forwards the onion to 3 which now looks like figure 3 and is represented as

E3PU ((5's IP ADDRESS, (E5PU (recipient's IP address, data))))

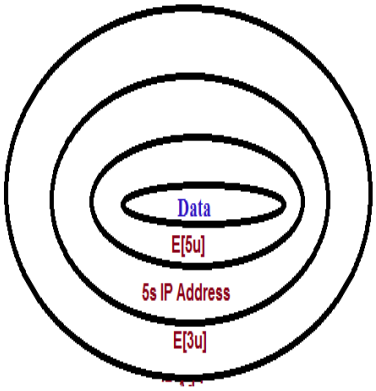

Figure: 3 Intermediate Node 4 Peels the Outer Layer of the Onion using its Private Key

Onion router 3 peels the outer layer of the onion using its private key. It forwards the onion to 5 which now looks like figure 4 and is represented as (E5PU(recipient's IP address, data)).

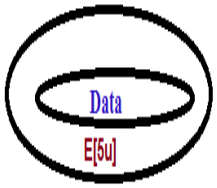

Figure: 4 Intermediate Nodes 3 Peels the Outer Layer of the Onion Using Its Private Key.

Onion router 5 peels the outer layer of the onion using its private key as represented in Figure It finds the plain data and the destination address and forwards it to the destination.

Figure: 5 Intermediate Node 5 Peels the Outer Layer of the Onion using its Private Key.

The size of the onion reduces as it nears the destination. Subsequently attackers can derive the details about the destination. To avoid this onions are padded at each onion router to maintain the size of the onion. Every onion routers has details of only its previous and next hop. So even if an onion router has been compromised the attacker can get only the encrypted onion. The attacker will not be able to decrypt the onion without the private keys and hence will not infer any valuable information from it. How the encryption and decryption process takes place.

d. ENCRYPT THE DATA

```
encryption(hdr->data);
send(pkt, 0);
return (TCL_OK);
}
else if (strcmp(argv[1], "start-WL-brdcast") == 0) {
Packet* pkt = allocpkt();
hdr_ip* iph = HDR_IP(pkt);
hdr_security_packet* ph = hdr_security_packet::access(pkt);
strcpy(ph->data, "test");
iph->daddr() = IP_BROADCAST;
iph->dport() = iph->sport();
ph->ret = 0;
send(pkt, (Handler*) 0);
return (TCL_OK);
}
else if (strcmp(argv[1], "oneway") == 0) {
oneway=1;
return (TCL_OK);
}
}
(Agent::command(argc, argv));
}
```

Encryption Function voidSecurity_packetAgent::encryption(char out[])

```
{
int key =3;
inti=0;
for (i=0;i<strlen(out);i++)
{
out[i]=(out[i]^key)%256;
}
}
```

Decryption voidSecurity_packetAgent::decryption(char out[])

```
{
int key =3;
inti=0;
for (i=0;i<strlen(out);i++)
{
out[i]=(out[i]^key)%256;
}
```

e. DECRPTION FUNCTION

```
unsignedintSecurity_packetAgent::hashing(char value[], unsigned intlen)
{
char *word = value;
unsignedint ret = 0;
unsignedinti;
for(i=0; i<len; i++)
{
int mod = i % 256;
ret ^=(unsigned int) (word[i]) << mod;
ret ^=(unsigned int) (word[i]) >> (256 - mod);
}
return ret;
}
```

f. PERFORMANCE EVALUATIONS

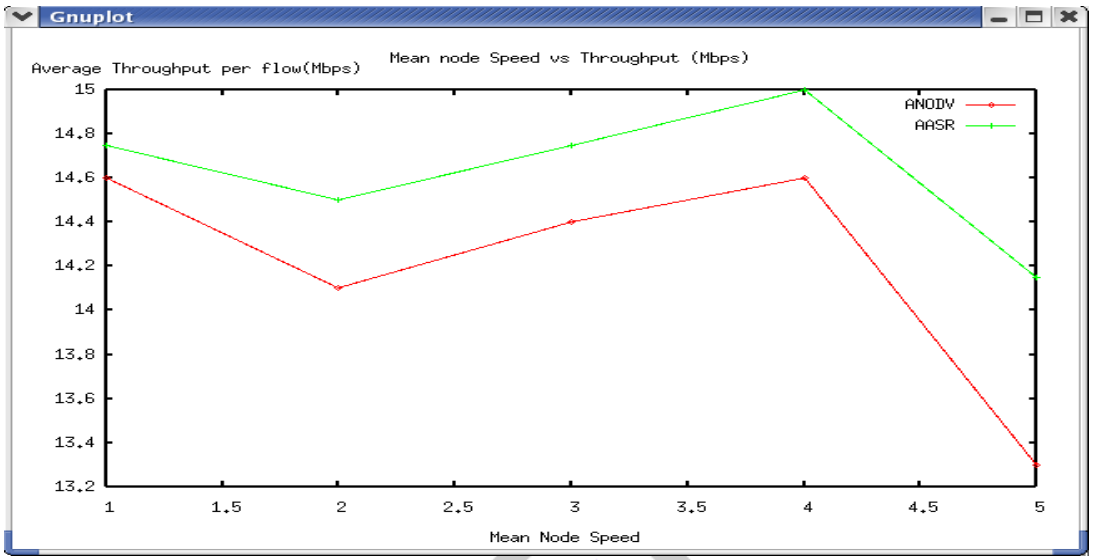

Figure 6 Throughputs

The figure 6 represents the performance analysis for the throughput between the two protocols ANODV and AASR. So it is found that the average throughput of ANODV decreases obviously when compared to the AASR protocol.

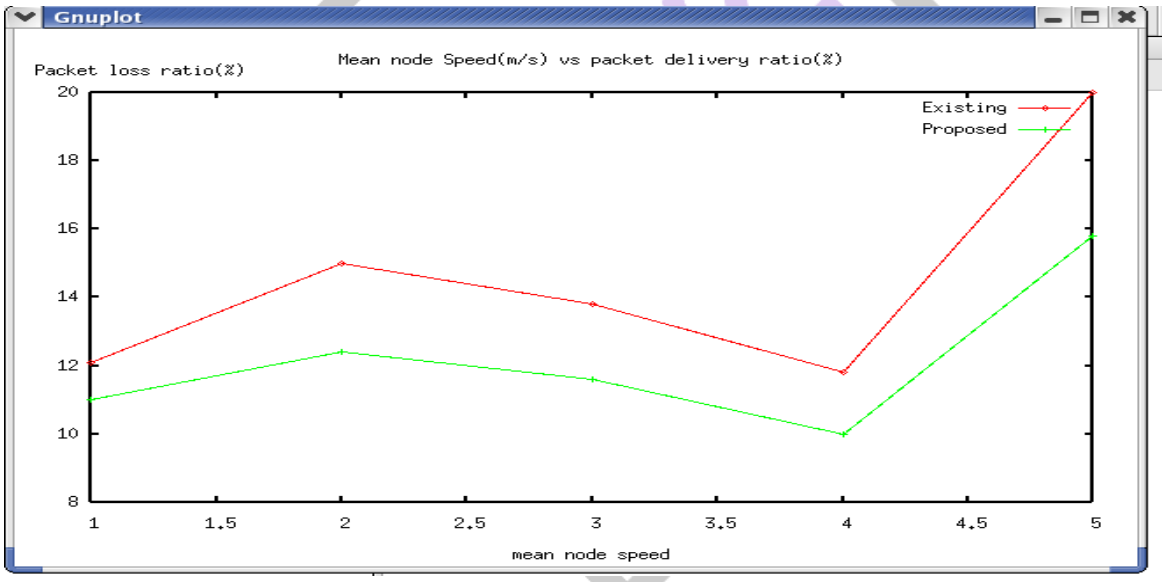

Figure: 7 Packet Loss Ratio

In this figure 7 the existing protocol ANODV is compared with the AASR protocol for the packet delivery ratio and found that the ANODV protocol has higher packet loss ratio then AASR protocol.

IV.CONCLUSION

An Authenticated and Anonymous Routing Protocol for MANETs have been designed in adversarial environments. In this protocol the route request packets are authenticated by group signatures, to defend the potential active anonymous attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message is designed not only to record the anonymous routes but also to prevent the intermediate nodes from inferring the real destination. Compared to ANODR, AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. In future work, this AASR will be improved to reduce the packet delay by combining it with a trust based routing. With the help of the trust model, the routing packets will be more dynamic in distinguishing link failures, caused either by the mobility or adversary attacks.

REFFERENCES

[1] Wei Liu and Ming Yu," AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" IEEE Transactions on Vehicular Technology, Volume: PP,Issue:99,Date of Publication, November 2014
[2] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in Proc. ACM MobiHoc, Jun. 2003, pp. 291–302.
[3] 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. IEEE Int. Conf. LCN, Nov. 2004, pp. 618–624.
[4] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop SASN, Nov. 2005, pp. 33–42.
[5] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 5, no. 9, pp. 2376–2386, Sep. 2006.
[6] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. SECURECOMM, Aug. 2006, pp. 1–10.
[7] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, Sep. 2011.
[8] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks," Int. J. Wireless MobileComput.,vol.3,no.3,pp.145– 155, Oct. 2009.
[9] B.Bhargava,"AO2P:Adhocon-demandposition-based private routing protocol," IEEE Trans. Mobile Comput., vol. 4, no. 4, pp. 335–348, Jul./Aug. 2005.
[10] H.Shen andL.Zhao, "ALERT:Annonymous location-based efficient routing protocol in MANETs," IEEE Trans. Mobile Comput., vol. 12, no. 6, pp. 1079–1093, Jun. 2013.