International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 21 (2015) pp 41859-41863

Secure And Efficient Route Trust In Mobile Ad Hoc Networks

Sameer Asayh[1], Rajeev Paulus[2]

[1]Research Scholar, [2]Assistant Professor [1, 2] SHIATS Allahabad, India
[1]sameerasayh@yahoo.ca, [2]rajeev.paulus@shiats.edu.in

ABSTRACT:
Although there are a large number of papers on secure routing in mobile ad-hoc networks, only a few consider the anonymous communication. In this paper, we define more strict requirements on the inscrutability and security properties of the various protocol, and notice that earlier works only provide Weak Localization based and mobile node traveling routes are discernible, and are vulnerable to specific attacks. Even though there are members of protocols which stresses on security of routing, no satisfying throughputs have been attained, most of the existing protocol are not strongly guarded against the ambush of counterfeit packets or denial of service. Therefore, in this paper proposed the modified onion routing protocol is presented, which concentrates on the defense against attack. This proposed protocol is termed as authenticated secure routing, i.e. Identity, confidentiality and geo-locality and ensure the place of safety to bare routes against various passive and active attacks. We intend to design a routing protocol which can protect the privacy of nodes and routes, and at the same time ensure the security of discovered routes. The purpose of this system is to motivate the participating nodes not only to help each other relaying data traffic, but also identify the median nodes, and to truncate them for the period of the route founding and increasing the route's security and reliability. Hence, an anonymous and secure route path can be established. Additionally, it has better characteristic for defending the Modified Onion Routing protocol improves the performance & efficiency through our simulation.

Key Terms: Secure Data Transmission, MANET, Modified Onion Routing, Homomorphic Encryption

Introduction:
Open wireless medium & dynamic topology are two of many attributes that cause peril and make the MANET's vulnerable in nature. In a rival environment i.e., battlefield it is strenuous to bestow assured and secure communication. There are two issues which can arise; one can be nemesis trying to gather information about the nodes or by following the traffics [1]. The other nodes of inside network turning malicious due to the influence of the nemesis. Hence anonymous communication is to be implemented which would conceal the routes and identifications [2], giving only random no's of instead of the actual information.
Anonymous is the feature which encloses details to one self making it unidentifiable or incognito MANET's two by trait that anonymous communication has is unidentified ability and unlink ability. Unidentifiable symbolizes that the traffic & route between any two nodes cannot be realized[3]. A number of routing protocol using anonymity was presented in last few years. The main focus here is on the topology which is based on demand anonymous and routing protocol. In order to reinforce the anonymous protocol [4] approaches are implied to anoymize the on-demand Adhoc routing protocols. Thus source, destination are the median nodes are to be anoymize to complete the process. Some of the results include protocols such as ANDOR [5],[7].
After analyzing and receiving the protocols it can be observed that unidentifiably and unlinkability are not wholly contented. For ex: modified onion routing protects only the route identities during the time of route discovery process. It also embraces a global trapdoor message this can be used to retrieve the intermitted nodes by Route Reply and forwarding[6]. Another example is SDAR where nodes each other know their ID's causing the whole process of anonymity in vain. In DSR, the destination node can be predicted by the median nodes. These protocols are also weak to DOS[7][8]. It is hard to identify if anode is malicious or not due to the absence of packet authentication. Hence a new method is launched as group signature. It follows the encrypted onion mechanism.
The paper is structured as follows. Section II contains the background and related work followed by network scenario in section III. Section IV presents the design of ASR and the evaluation is done in v and results of simulation are provided.

II. Background and related work.
The groundwork of anonymous routing and a look at the existing protocols are seen in this section.

II a).ANONYMITY AND SECURITY PRIMITIVES.
a-1). Trap door:
Trapdoor is a cryptographic function which defined a one way function between 2 sets. A global trapdoor may be defined as a collection of information in which the median nodes can contribute to the data by adding a data such as node 10's. The retrieval of these data can be done only by the source and destination node which can lock and unlock the trapdoor. This requires an end to end key.

a-2). Onion routing:
It is a technique which renders private communication over a public network. The core is set by the source which holds a specific route message. The other nodes are added as layers and encrypted. The node of destination receiver the onion and forward it's back to the source. The media nodes decrypt the layers and by this process anonymous route can be corroborated.

a-3). Group signature:
This is a process which authentically the packets without interrupting the anonymity. A presented the all members of the group with 2 sets of key-public and private by the group manager. Each node signature is is defined as its privative key which is verified by other members. Only the group manager can track the signer's identity.

b). ANONYMOUS ON DEMAND ROUTING PROTOCOLS:
A number of anonymous on-demand routing protocols which be classified into

i). topology-based or node identity centric and
ii). Location –based or location centric.

Table I contains key distribution, assumptions, node i nonymity and packet authentically. These features are compared and the 3 following observation is made

1). Each routing protocol is developed to work in a particular scenario. Not are protocols prosper well is all the situations.
2). Unidentiabilty and unlinkability are likely to be lost during the routing process. This makes the process less anonymous causing the intruders to attack more easily.
3). Two protocols adopt excess authentication scheme to sign the routing packers. Developing a master key is done, which does not provide anonymity or enforcipity. Onion based routing is commonly used as it is more scalable and can extends multiple paths.
4). A process must be newly developed for key distribution which can be advance share. This contributes more security.

c. Network scenario:
This section argues regarding the attack and adversaries models in the network and node model.

c-a). Adversaries and attack models:
A basic notion is made that the adversary has all the information about the network protocol and its function. To know, the chance of attacks outside the secret key is less compared to ones inside the network. The classification of behavior the attacks as active and passive of abased on the location they are organized as inside and outside.

i. Passive outside attack:
Observation and recording of the entire network takes place by outside. They collect information about node identifies destination, sources and routes.

ii. Active outside attack:
The main goal is to disrupt the routing or initiate a DOS. They are very dangerous as they can project attack from any place randomly. They don't have the need to be invisible unlike passive outside attack.

iii. Passive inside attack:
From the network, the nodes are attacks try to collect information about the source and destination without revealing themselves.

iv. Active inside attack:
These attacks have the power to modify, inject and replay messages and can also initiate attacks. They can cause a lot of damage.

D. Network assumptions:
MANET is denoted as Manet_T and the following assumptions are made:

1). Public key infrastructure:
A pair of public key and private key provided by a public key infrastructure (PKI) (for each node T) or other certificate authority C(A). the denotation of public\private key can be done as follows:
For node $A(A \in T)$ and K_{A+} and K_{A-}

2). Group Signature:
An assumption is made that the entire network Manet_T as a group and all of the nodes present in the network has a couple of private and public key, which is provided by the group manager. G_{T+} denotes the public key which is same for the entire group. G_{A-} denotes the private key which unlike public key is different for each node.

3). Neighborhood symmetric key:
A key which is created by two nodes in a neighborhood by security association is called symmetric key. And it is shared and denoted as K_{AB} for 2 node i and j $(A, B \in T)$.

C). Node model:
1). Destination Table:
All the possible destination nodes are in the knowledge of the source node is an assumption made. Destination table contains all possible information destination information like destination pseudonym, public key etc. the symmetric key is needed to encrypt the data after the destination is determined.

2). Neighborhood Table:
The symmetric key which is shared by the nodes locally in order to transfer information and generate types is pseudonyms are stored in this table.

Notations	Descriptions
NA	One-time Nym. generated by A to indicate itself
(d)KA	Data d is encryp. by one symmetric key of A
{d}KA+	Data d is encrypt. by key KA+
GA	Group private key of node i
d KAB	Data d is encrypt. by shared key KAB
KAB	Symm. key shared by node i and j
GT +	Group public key of network T
KA	Private key of node i
OK (m)	Encryp. onion for message m with key K
[d]KA	Data d is signed by node i
KA+	Public key of node i

3). Forwarding table:
Route records about switching information are stored in the table. A route pseudonym is induced by the destination node during each entry in the table.

4).Routing Table:
The routing table holds request pseudonyms and the secret verification message. A new entry is created every time a node is generated or forwarded. These are two stages\states in this table. Active and pending. Active is used to denote the complete upadation, which pending the opposite of it.

III) PROTOCOL EVALUATION:
This section involves the evaluation of ASR and its defense.

A). Anonymity analysis:
There are basically three types of anonymity. An assumption is made that every node even on the discovered route are nemesis and are eager to discover the route and information. The types of anonymity are as follows.

1). Identity anonymity:
There is the interconnection between the functioning of nodes and their identities. The node can operate without ids. All the nodes initiate so that the source and destination identities cannot be discovered. In RREQ packet only trap door information is preset.
But is modified onion routing, Route Replies uses test in backward forwarding. This can be used to figure out the destination node with the help of malicious intermediate nodes. In order to prevent this from happening encryption table place.

2).Route Anonymity:
The nodes have information only about the previous and next pseudonym. Hence the discovery of the route is tough as there is no proper information. The destination pseudonym is on time randomly generated which makes it difficult for the intruders to know the entire route.

3). Location Anonymity:
There is nice information about the topology and the number of nodes in a network. Hence even with the help of a malicious node inside the network it is impossible to discover the network topology.

B). Security Analysis:
1). Passive attack:
Global eves dropping are a major passive attack. Identity information about the source or the destination is impossible to retrieve from this type of attack.
Silent dropping is another example for passive attacks. This process involves selfish nodes which refuse to do its functionality in the protocol.
Watch dog model is established to protect against these type of passive attack in the routing. But it is tricky to identify selfish nodes and malicious node in a anonymous network.

2). Impersonation attacks:
These types of attacks are caused due to inside is attack. In RREQ any node can modify the message and forward it. But in ASR it is impossible to modify. No node can join the network without the group key. Due to the fact that the duplication of the signature is not possible.

3).DOS Attack:
The main aim of DOS is to deplete all the resources from the node. If the attack is launched from the outside very little damage can be done as they do not possess the keys. But if the attack is done from the inside a large amount of requests will be sent to the route causing an abnormal behavior. This will be detected by the group manager and the attack will be identified b tracking the signature used.

IV) Performance simulation:
This section compares the performance of ASR to the other pre-existing secure routing algorithms.

A). network configuration:
1). Topology and traffic:
For simulation a area of 1500 m X 1500m is chosen with 18 nodes equally distributed. MAC layer is formed using DCF of IEEE 802.11. A channel of capacity 2Mbps is used. Transmission range is set to be 250m. Random way point is used for Node mobility. Speed various from Max to Min range n simulation. In order to generate traffic 15 UDP based CBR are used totally. Data packets of 512 bytes are created for each session. Source and destination pair is chosen by a random process.

2).Attack models:
An assumption is made that median nodes can turn malicious. It will randomly drop packets. It probability ranges from zero to eight.This is designed to give different levels of attack in the simulation. Due to lack of authentication modified onion routing, AODV suffer the damages more compared to ASSR. ASR has authentication and can also trace the malicious node with the signature and get rid of it.

B). Simulation Result:
Two groups of results are presented one a comparison between pre existing routing algorithms Vs ASR. Another group to compare the behavior palter under different levels. Approximately best simulation configuration, performance and loss ratio are recorded.

Group 1: The effect of mobile scenario:
In order to set the adversarial environment 10% of the total nodes are set malicious mobility of the networks is changed from 1 to 5 m/s.
From the observation it is found that the average speed increases in the nodal mobility. Despite performance variance, ASR always achieves the highest throughput.fig 2(a) and 2(b) shows the throughput and loss ratio of ANORD and ADDV. It is observed that they are similar. It can also be observed that AODV & Modified Onion Routing have longer delays due to external security issues. Whereas ASR has less than 40ms

delay than their average.

2) Group2: effect of malicious attacks

The average speed of mobiles n/w is configured to 10 m/s. The malicious node, range from 0 to 9. it helps to notice the obvious that where the malicious nodes increase, the other pre existing protocol decreases. But ASR has less loss ratio. It is due to the fact that it can detect and get rid of the malicious nodes. The end to end delays are higher in ASR & Modified Onion Routing due to the security process. While AODV does not acknowledge malicious nodes there is no delay. When the attack is very high in Modified Onion Routing it retours which causes higher delay. Hence it can be concluded that ASR is 40 ms less of delay in average compared to Modified Onion Routing.

IV Results and discussion

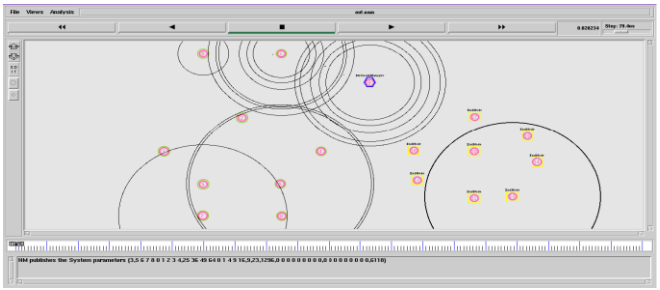


Fig1. Represents that network parameters publishes the system parameters with different values.

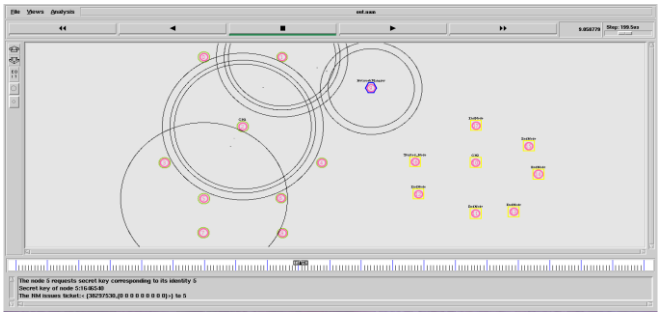


Figure 3 indicates the node5 is request the secret key corresponding node identity.

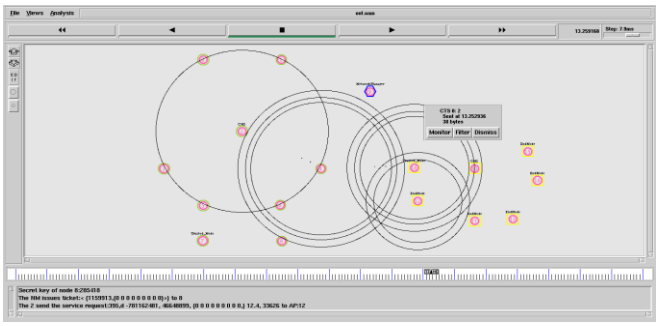


Figure 2 indicates that secret key of node 0 is set 285418 and network manager issue the ticket to node 8, during that time node 2 is send the request to AP 12.

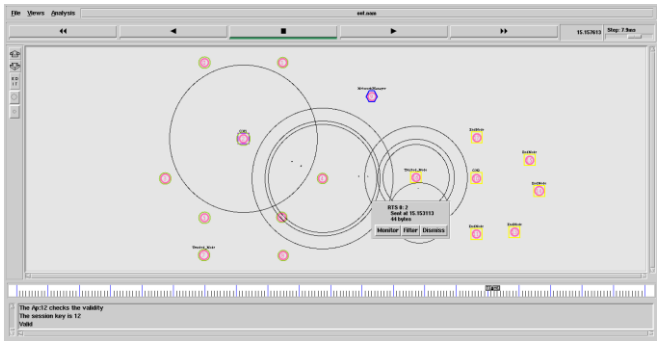
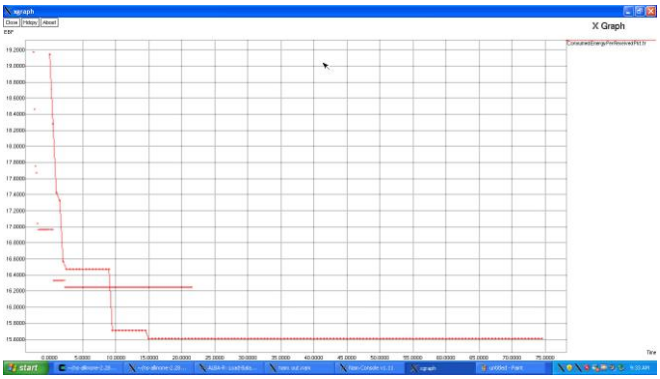
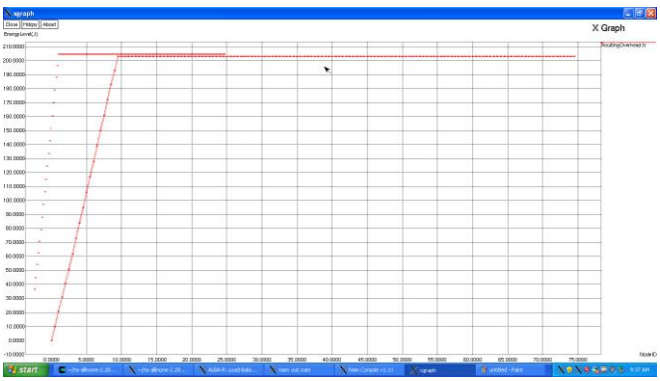


Figure 3. indicates the AP12 ensures the validity and the session key is 12 is valid.

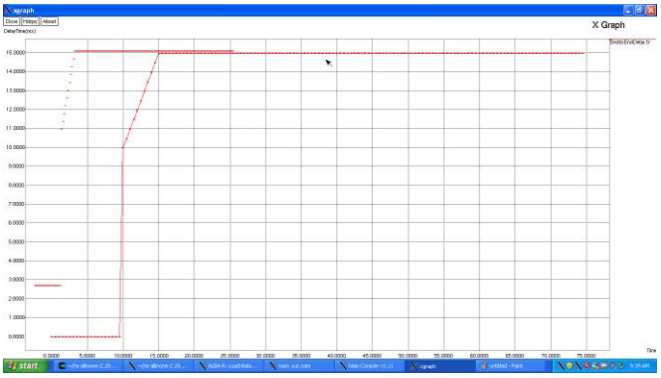
The above graph describes about the packet delivery ratio.



The above graph describes about the consumed energy per received packet.



The above graph describes about the routing overhead.



The above graph describes about end to end delay.

V Conclusion

A new secure homomorphic protocol is designed with the key feature as authentication & anonymity. It is highly useful in the old revisal environment. Authentication of group packet by signature is established to defined and secure the nodes identities. Verification of message is done through secure hash key encryption. Hence all security measures are enhanced in this routing process enabling detection & prevention from attackers. Better efficiency, scalability & mobility are also found in ASR. It is effective compared to the rest of the pre existing secure routing.

VII References

[1] Weisong Shi, Guoxing Zhan, and Julia Deng. "Sensortrust: A resilient trust model for wireless sensing systems. Pervasive and Mobile Computing", 2011.

[2] Ramona Rednic, John Kemp, Elena Gaura, and James Brusey. "Networked body sensing: Enabling real-time decisions in health and defence applications". In Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on, pages 17 –24, dec. 2011.

[3] W. Shi, G. Zhan, and J. Deng. "Tarf: A trust-aware routing framework for wireless sensor networks". In Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 2010.

[4] W. Shi and L. Liu. "Trust and reputation management". Internet Coomputing, 14(5), sep/oct 2010.

[5] Chen, Z. You, X. Zhao, W. GongDand, K. Lam and M. Gu,. "Trust based routing for misbehavior detection in ad hoc networks". Journal of Networks, 5(5), May 2010.

[6] John Krumm, A.J. Bernheim Brush, and James Scott. "Exploring end user preferences for location obfuscation, location-based services, and the value of location". In Proceedings of the 12th ACM international conference on Ubiquitous computing, Ubicomp '10, pages 95–104, New York, NY, USA, 2010. ACM.

[7, A. Sharma, R. Ramjee, T. Das, V. Padmanabhan and P. Mohan. "Prism: Platform for remote sensing using smartphones". In Proceedings of the 8th international conference on Mobile systems, applications, and services, MobiSys '10, pages 63–76, New York, NY, USA, 2010. ACM.

[8] L. P. Cox and L. Deng. Livecompare: "Grocery bargain hunting through participatory sensing". In HotMobile '09: Proceedings of the 10th workshop on Mobile Computing Systems and Applications, pages 1–6, New York, NY, USA, 2009. ACM.

[9] Z. Chen, J. Hu,, M. Xu, Z. Cao,and X. Zhou. "Fbsr: Feedback-based secure routing protocol for wireless sensor networks." International Journal of Pervasive Computing and Communications, 2008.

[10], Jr-ben Tian,, Hao-Hua Chu, Polly Huang and Ho-lin ChangTsung-Te Lai." Spinning beacons for precise indoor localization". In Proceedings of the 6th ACM conference on Embedded network sensor systems, SenSys '08, pages 127–140, New York, NY, USA, 2008. ACM.