ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Enhanced Secure Group on-Demand Routing Protocol for MANET

Shafna V.S.M, Alamelu Mangai. M, Dr.R.Deepa,

Department of ECE, Nehru Institute of Technology, Coimbatore, India.

Department of ECE, Nehru Institute of Technology, Coimbatore, India

Department of ECE, Nehru Institute of Technology, Coimbatore, India

Abstract: MANET doesn't need a set network infrastructure; each single node works as each a transmitter and a receiver and they trust their neighbors to relay messages. Unfortunately, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. In this project, we define solid privacy requirements regarding malicious attackers in MANET. There are so many existing research work proposed a implementation of new intrusion-detection systems. Existing works demonstrated the higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. But the problem is most of the systems are on-demand manner, that means after the attack only detection will be done. These methods may help to civil application, but in defense application existing system won't provide much security. So we proposed a method with incorporated digital signature with group ID and Routing packets. By our method we can avoid the INTRUDERS.

KEY WORDS*:* Security, MANET, Routing, USOR.

I.INTRODUCTION:

MANET may be a network that is freelance network. As a result of figureless property, network could also be laid low with attackers. To avoid security drawback there are several numerous researchers fictional many security strategies like encoding strategies. To enhance security here we have a tendency to mistreatment standard 2 strategies, one is RSA formula and Sha-1 formula. During this project we have a tendency to prompt un-observability by providing protection for the asking and reply. Our proposed system main aim is to provide ultimate security in military application

Fig.1 MANET devices in ARMY

II.LITERATURE SURVEY

In this paper [1], author specialize in a specific category of flow correlation attacks, traffic analysis attack, by that associate opponent attempts to research the network traffic and correlate the traffic of a flow over an input link at a combination thereupon over an output link of a similar mix. Analyzing of combine networks was worn out terms of their effectiveness in providing obscurity and quality-of-service and it shows that it are able to do a secured low detection rate whereas maintaining high outturn for traditional payload traffic however unlinkability alone isn't enough in hostile environments like battlefields as necessary data like packet sort are still accessible to hackers. Then a passive offender will mount traffic analysis supported form of packet. In this paper [2], author proposes a completely unique anonymous on-demand routing protocol, named MASK, to modify anonymous communications thereby thwarting doable traffic analysis hackers. supported a brand new crypto graphical construct referred to as pairing, he initial proposes associate anonymous neighborhood authentication protocol that permits neighboring nodes to attest one another while not revealing their identities. A pairing primarily based anonymous on-demand routing protocol MASK is that provides robust sender and receiver anonymity, the link obscurity between receivers and senders, the un-locatability of mobile nodes and also the un-traceability of packet flows underneath a rather robust adversarial model however the routing data isn't documented within the current style of MASK. In the paper [3], author proposes a totally self-organized public-key management system that permits users to come up with their public and personal key pairs, to publish certificates and to perform authentication notwithstanding the network partitions and with none centralized services. Moreover, this approach doesn't need any trustworthy efficiency, not even within the system data format part. Self-organized public-key management theme is planned that doesn't have confidence any trustworthy authority or outlined server, not even within the data format stage. Author showed that with a straightforward native repository construction formula and a tiny low communication overhead, this technique achieves high performance on a large vary of certificate graphs however it needs users acutely aware involvement only their public/private key pairs are created and for provision and revoking certificates.

In this [4] paper, author develops associate untraceable routes or packet flows in associate on-demand routing atmosphere. This aim is extremely completely different from alternative connected routing security issues like resistance to route disruption or bar of denial-of-service attacks. Associate anonymous on-demand routing protocol ANODR for mobile impromptu networks deployed in hostile environments. It demonstrates that untraceable information forwarding while not encrypted routing header are often with efficiency accomplished however main disadvantage of this mechanism is that every one nodes receiving the RREQ message should try and decipher the worldwide trapdoor to search out whether or not it\'s the supposed receiver, succeeding in appreciable overhead. [5] During this paper, author proposes associate Anonymous Secure Routing protocol that may offer extra properties on anonymity, i.e. Identity obscurity and robust Location Privacy, at a similar time make sure the security of discovered routes against varied passive and active attacks. The Anonymous Secure Routing protocol is planned that provides a lot of obscurity and security to the mobile ad-hoc networks that was a disadvantage in previous protocols however within the cases of route changes or link failures some issues can arise during this protocol.

III.SYSTEM ANALYSIS:

A. Existing system:

A number of secure routing define are brought forward MASK relies on a special form of public key crypto system and also the pairing-based cryptosystems are to realize anonymous communication in MANET.

B.Disadvantages:

Existing schemes fail to guard all content of packets from hackers, in order that the offender will get information like packet sort and sequence numbers etc. These details are often wont to relate 2 packets that break unlinkability and will cause supply trace back attacks.

Another disadvantage of previous outlines is that they bank heavily on public key cryptography and so incur a awfully high computation overhead.

IV.**PROPOSED WORK:**

In this project, we have a tendency to introduced associate economical privacy maintain routing protocol USOR that achieves content un-observability by using anonymous key institution supported cluster signature.

A.Advantage:

This project is implementing high security information transfer therefore we will avoid hacking in contrast to information security, it providing the fundamental packet security additionally.

B.Proposed system description:

During this project, we have a tendency to outline solid privacy necessities relating to privacy-maintain routing in MANET. We have a tendency to propose associate imperceptible secure routing theme USOR to supply complete unlink ability and content un-observability for every kind of packets. USOR is economical because it uses a completely unique combination of cluster signature and ID-based encoding for route discovery. The simulation results show that USOR not solely has satisfactory performance compared to AODV, however additionally achieves stronger privacy protection than existing schemes like MASK

V.MODULES:

- Basic routing module
- Insert hacking in basic routing module
- Secure Acknowledgement
- MRA

A.Basic Routing Module:

If the source has no route to the destination, then source v initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node.

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

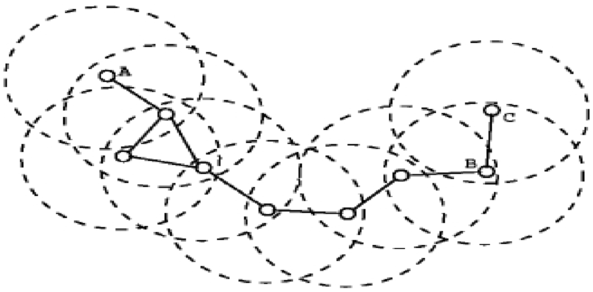


Fig.1 Basic Route Discovery

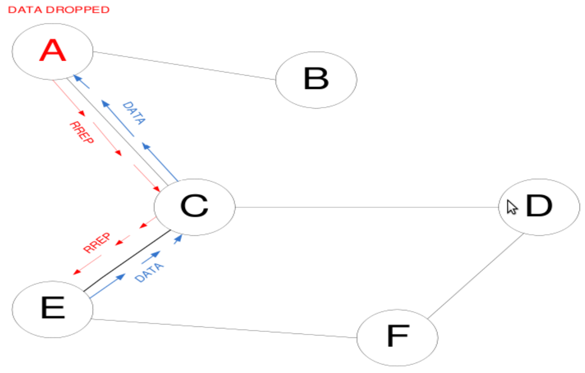
B.Include Hacking In Basic Routing Module:

In this module Attack issues will arise in to the network. Providing security to the attacks will be considered.

BLACK HOLE ATTACK:

MANETs face different securities threats i.e. hack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET).

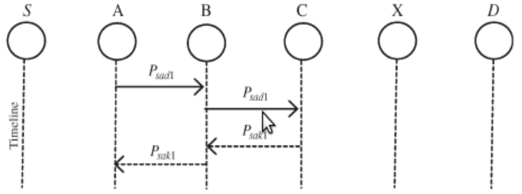
In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to include. This hostile node advertises its availability of fresh routes irrespective of checking its routing tables. In this manner attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.



c.protected acknowledgement:

- In this module, we are implementing secure acknowledgement to detect misbehaving nodes in the routing environment.

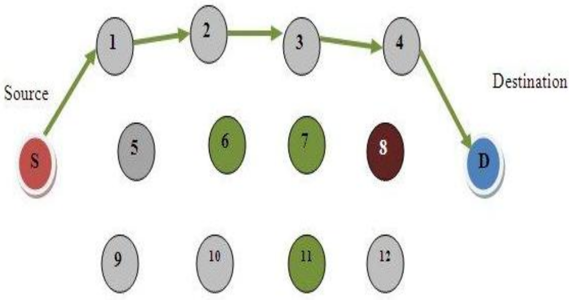
- In this module we are ensuring that acknowledgement is authentic and untainted by Digital Signature.



In the above figure S is the source node whenever it doesn't receives the acknowledgement it will start secure acknowledgement process within three-three nodes. Here A, B, C is the 1st group which node A sending one packet to node B, it will forward to node C after that both nodes B and C have to send acknowledgement to node A within time. If acknowledgement not received means it will report those nodes as misbehaving nodes to source node. But in this process there is a chance of false reports to avoid this we are implementing MRA.

D.MRA:

- In this module we are avoiding false reports generated by the Misbehaving nodes.
- The main aim of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.



In the above figure we can observe that between source and destination there are multiple paths available in MANET. So, to avoid false reports in secure ACK scheme we will find another path between source and destination and source will check the reports which it gotten from intermediate nodes if any false report found means it will treat the node which sent that report as a misbehaving node.

VI.UN-OBSERVABILITY IMPLEMENTATION:

Algorithm for USOR:

```
1. Initialize the nodes as follows
   a. Leader node: (it will share the key at initial time)
   b. Normal node: (normal mobile node)
2. Leader node will send the cluster ID key to any or all then mobile node
3. If traditional node received that ID then stores into memory
4. If node having GID
   a. It will access the request
5. If not
   a. can't access the request
6. If node (i) desires to speak with another node
   a. Node i generates the hash code (by sha-1)
   b. Encrypting (by RSA) that code with personal key of nodei
   c. And sends to destination node
7. Destination node will verify that encrypted message by mistreatment the general public key and moreover as cluster ID
   a. if match
      i. node j causation own code to supply node i
   b. if not match
      i. ignore
8. if match code of node j
   a. transfer the data
9. if not match
   a. ignore
```

A.ANALYSIS

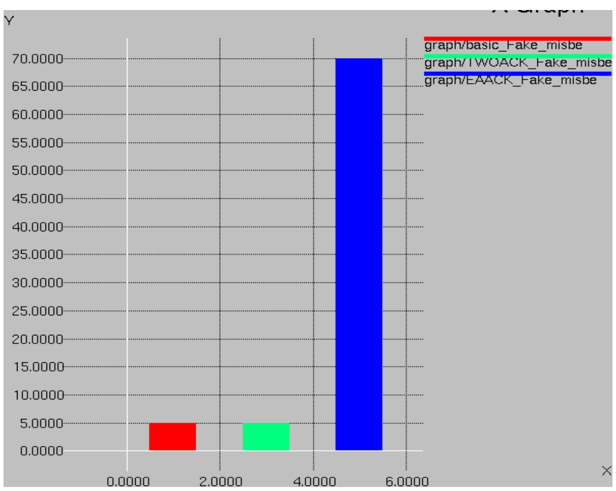
Network performance refers to the service quality of a communications product as seen by the client. There are many various ways that to live the performance of a network, as every network is completely different in nature and style.

Packet delivery performance

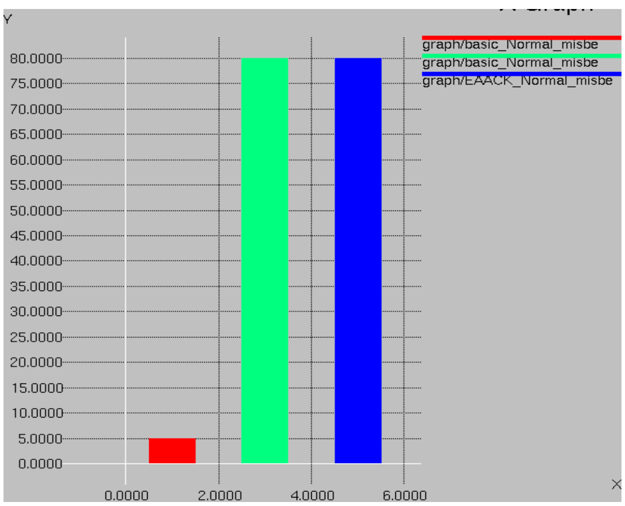
PDF is that the term wants to live the network performance. PDF defines the what quantity packet delivered properly over total variety of packet sent

Overhead

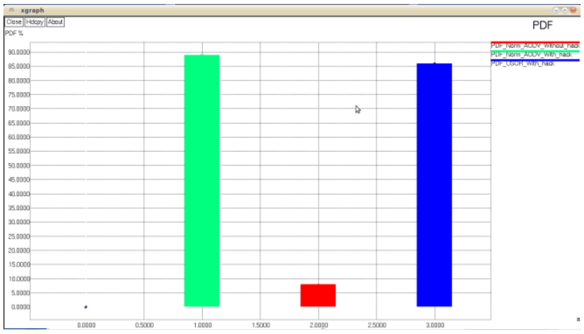
Overhead is that the one necessary construct to investigate network performance. Overhead is outlined as variety of routing and management packet is requiring transferring the info.



Graph.1 PDF while fake acknowledgement (green TWO-ACK, Red- BAODV, Blue-Proposed system)



Graph.1 PDF while basic malicious environment (green TWO-ACK, Red- BAODV, Blue-Proposed system)



VII.CONCLUSION:

In this paper, we have a tendency to prompt associate imperceptible routing protocol USOR supported cluster signature and ID-based cryptosystem for impromptu networks. The conception of USOR offers solid privacy protection complete unlinkability and content unobservability for impromptu networks. The protection analysis demonstrates that USOR not solely provides robust privacy protection; it's additionally a lot of resistant against attacks as a result of node compromise. We tested successfully worm-hole attack in our method.

ACKNOWLEDGMENT

We would like to acknowledge the efforts of ***Pantech ProEd Pvt ltd., India***, for steerage that helped us work effortlessly towards manufacturing this scientific research work.

REFERENCES

[1]“*On Flow Correlation Attacks and Countermeasures in Mix Networks”*, Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao - 2004.
[2]“*Anonymous Communications in Mobile Ad Hoc Networks*”, Yanchao Zhang, Wei Liu and Wenjing Lou - 2005.
[3]**“***Self-Organized Public-Key Management for Mobile Ad Hoc Networks*, Srdjan Capkun, Levente Butty Ì• n and Jean-Pierre Hubaux - 2003.
[4]“*ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks*”, Jiejun Kong, Xiaoyan Hong - 2003.
[5]“*Anonymous Secure Routing in Mobile Ad-Hoc Networks”*, Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng - 2004.
[6]”*ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks*, Stefaan Seys and Bart Preneel - 2009.

[7]“*SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks”*, Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba - 2004.

[8] “*ALARM: Anonymous Location Aided Routing in Suspicious MANET”**s***, Karim El Defrawy and Gene Tsudik - 2011.

[9] “*Identity-Based Encryption from the Weil Pairing”*, Dan Boneh, Matthew Franklin - 2001.

[10] “*SybilGuard: Defending Against sybil Attacks via Social Network”**s***, Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman - 2006**.**