IJRRECS/October 2013/Volume-1/Issue-6/1366-1373 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN OF SOLID HYBRID SECURITY PROTOCOL FOR MANET IN MILITARY APPLICATION

Bajjuri Naveen[1], Maheswara Reddy Sura[2]

[1]M.Tech (DECS), Dept of ECE, Gurunanak Engineering College, Ibrahimpatnam Hyderabad, A.P, India Email: naveenbbc.08@hotmail.com

[2]Professor, Dept of ECE, GuruNanak Institutions Technical Campus School of Engineering and Technology, Ibrahimpatnam, Hyderabad, A.P, India

ABSTRACT:

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

Keywords: Security, MANET, Routing, solid hybrid security protocol.

1. INTRODUCTION:

MANET may be a network that is freelance network. There is MANET technology used in different application, like military and civil applications. 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

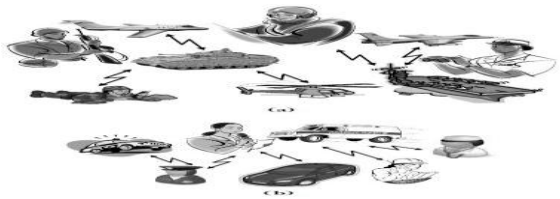

Fig.1a MANET devices in ARMY, b) MANET in civil application

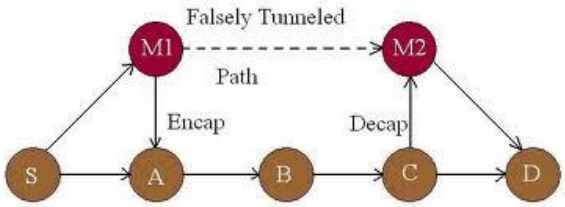

Fig.2 wormhole attack

In a wormhole attack, hackers are tunneled packets to another area of the network bypassing normal transmission routes as shown in Figure 2. In practice, hackers can use eminent power antennas or a wired link, or some other methods. This resulting route through the wormhole may have a meliorate metric, i.e., a lesser hop-count than normal paths. With this purchase, hackers using wormholes can easily fake the routing priority in MANET to perform dropping, packet. The entire routing system in MANET can even be brought down by the wormhole attack.

I. 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 this 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 paper [4], 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.

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.

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.

II. Proposed Work:

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

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.

Un-observability implementation:

Algorithm for Solid Hybrid Security Protocol:

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 node i
   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

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 solid hybrid security protocol to supply complete unlink ability and content un-observability for every kind of packets. Solid hybrid security protocol is economical because it uses a completely unique combination of cluster signature and ID-based encoding for route discovery. The simulation results show that solid hybrid security protocol not solely has satisfactory performance compared to AODV, however additionally achieves stronger privacy protection than existing schemes like MASK

Modules:

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

Basic Routing Module:

If the supply has no route to the destination, then supply initiates the route discovery in associate on-demand fashion.

After generating RREQ, node appearance up its own neighbor table to

search out if it's any nearer neighbor node toward the destination vehicle.

If a more in-depth neighbor node is out there, the RREQ packet is forwarded thereto vehicle. If no nearer neighbor node is that the RREQ packet is flooded to any or all neighbor nodes. A destination node replies to a received RREQ packet with a route reply (RREP) packet in barely the subsequent 3 cases:

1) If the RREQ packet is that the initial to be received from this supply vehicle.

2) If the RREQ packet contains a better supply sequence variety than the RREQ packet antecedently gone through by the destination vehicle

3) If the RREQ packet has a similar supply sequence variety because the RREQ packet antecedently gone through by the destination node, however the new packet indicates that a more robust quality route is out there.

Include hacking in basic routing module:

In this module we have a tendency to together with the hacking node with our network that the assaultive node creates drawback and currently we have a tendency to about to analyze our current network standing with some drawback and ready to solve it.

Protection against hacking:

In this module, we have a tendency to implementing solid hybrid security protocol by protective all data that explicit packet.

In this module the packet is known by approved users solely, alternative node can't determine data that packet.

1.1.1. Protection against hacking

In this module, we've a bent to implementing solid hybrid security protocol by protecting all knowledge that express packet.

In this module the packet is thought by approved users exclusively, various nodes can't confirm knowledge that packet.

In this we included digital signature method to make more secure transmission. For making Digital sign we can use cryptosystem technique.

There are four processes that are specific and essential to a pair wise key cryptosystem:

a) Decrypt an encrypted message gives you the original info, specifically

$$D(E(M)) = M$$

b) Reversing the process still returns M:

$$E(D(M)) = M$$

c) E and D are simple to compute.

d) The publicity of E does not concede the D secrecy, meaning you cannot simply figure out D from E.

Let e, d, n be positive integers, with (e, n) as the encryption key, (d, n) the decryption key, **n = pq**.

Now, we encrypt the message by raising it to the eth power modulo n to obtain C, the cipher text. We then decrypt C by raising it to the dth power modulo n to obtain M again. Formally, we obtain this encryption and decryption algorithms for E and D:

$$C \equiv E(M) = M^e mod(N)$$

$$M \equiv D(C) = M^d mod(N)$$

III. 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.

Result:

In our project, we have a tendency to analyzed completely different network atmosphere with main network parameters like packet delivery radio and overhead.

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

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

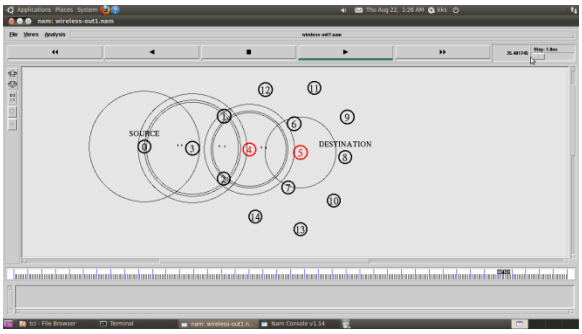

Fig.3 Wormhole attack in MANET

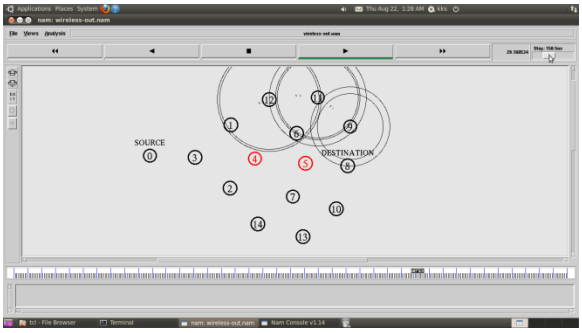

Fig.4 Prevention against wormhole attack by Solid Hybrid Security Protocol

Table1: performance comparison

Protocol	*PDF (%)*	*OH(pkt)*	*Delay(ms)*

AODV	88.926	306	38
Mali	8.2	305	410
SHSP	81	190	39

Result shown bellow is packet delivery performance. In this graph, there are the 3 atmospheres (without malicious environment, with malicious atmosphere and solid hybrid security protocol environment) shown.

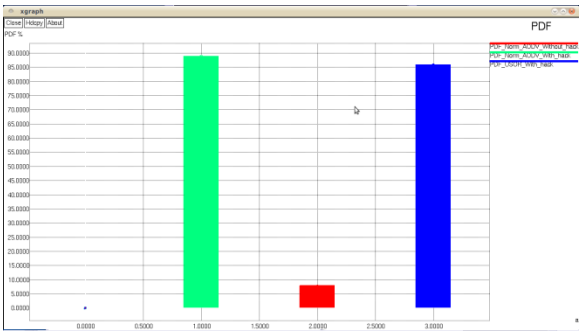

Fig.5 Packet delivery Comparison b/w AODV, Mali_AODV and solid hybrid security protocol

The graph shown bellow is overhead graph, from this result we will grasp solid hybrid security protocol has a lot of overhead than traditional AODV. Solid hybrid security protocol performance is best than traditional AODV even overhead is more; the rationale is security of solid hybrid security protocol is extremely high therefore overhead is ignorable during this case.

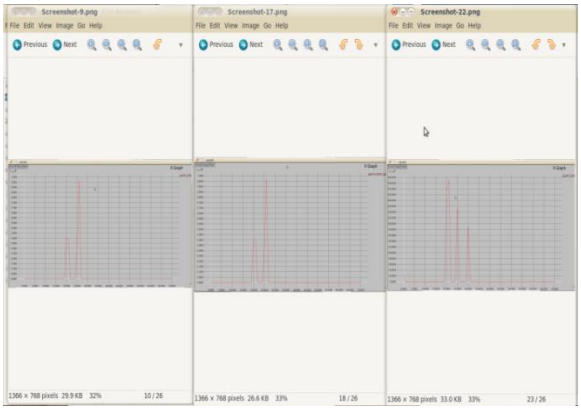

Fig.6 OH Comparison b/w AODV, Mali_AODV and SOLID HYBRID SECURITY PROTOCOL

IV. CONCLUSION:

In this paper, we have a tendency to prompt associate imperceptible routing protocol Solid hybrid security protocol supported digital signature and ID-based cryptosystem for impromptu networks. The conception of Solid hybrid security protocol offers solid privacy protection complete unlinkability and content unobservability for impromptu networks. The protection analysis demonstrates that Solid hybrid security protocol 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 this scientific research work. **http://www.pantechproed.com/**

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.

Bajjuri.naveen *is pursuing M.tech (DECS) in Gurunanak Engineering college ibrahimpatnam hyderabad in the accadamic year of 2011-2013. He intested on Mobile Ad-hoc network research.*