IJRRECS/October 2013/Volume-1/Issue-6/1339-1346 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN OF NOVEL AGITATION AODV ROUTING PROTOCOL FOR DEFENSE AGAINST BLACK HOLE ATTACK

T.Bhavana[1], M.Sowjanya[2]

[1]M.Tech (DECS), Sri Indu College of Engineering & Tech, Hyderabad, A.P, India

bhavanathota83@gmail.com

[2]Assist. Prof., Sri Indu College of Engineering & Tech, Hyderabad, A.P, India

sowjanya.maddireddy@gmail.com

ABSTRACT:

Military concerned about the security of information exchanges have always heavily relied on secure exchanges of short messages. Secure Message Transmission protocol secure the data transmission phase by tailoring an end to end secure data forwarding protocol to the MANET communication requirements and increases the reliability through transmitting the messages in multiple paths with minimal redundancy.

Keywords: Security, MANET, Multipath, military.

1. INTRODUCTION:

In the upcoming generation of wireless communication technology, there will be a need for the rapid deployment of independent mobile users. Substantial examples include establishing survivable, dynamic, efficient communication for emergency/rescue operations, military, and disaster relief effort networks. Such technology scenarios cannot rely on centralized and organized infrastructure, but can be conceived as applications of MANET. A Mobile Ad Hoc Networks is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless ties. Since the nodes are movable, the network topology may change rapidly and unpredictably over time. Technology is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes itself, i.e., the routing

functionality will be incorporated into mobile node.

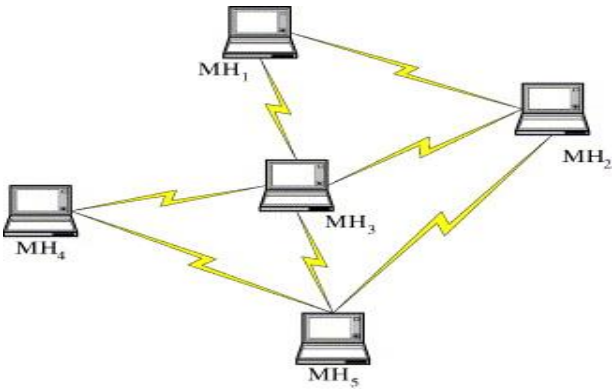

Fig.1 MANET Environment

1) Black Hole Attack

It is the basic Byzantine Attack where the adversaries stop forwarding the data packets but still participates in the routing protocol correctly.

Black hole attack: In a black hole attack, a hacking node sends fake routing information, arrogating that it has an optimum route and causes other good nodes to route data packets through the malicious one(fig.2). For example in AODV, the assaulter will send a pretend RREP (including a pretend destination sequence range that\'s invented to be equal or beyond the one contained within the RREQ) to the supply node, claiming that it's a sufficiently contemporary route to the destination node. This causes the supply node to pick the route that passes through the assaulter.

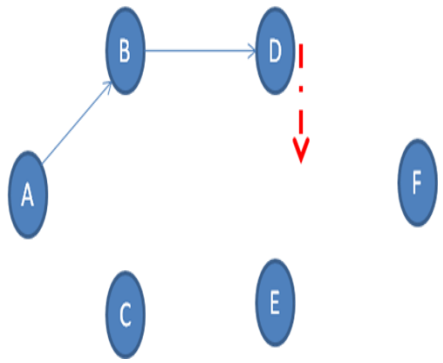

Fig2. Black hole attack

Therefore, all data will be routed through the attacker, and therefore, the hacker can misuse or discard the traffic

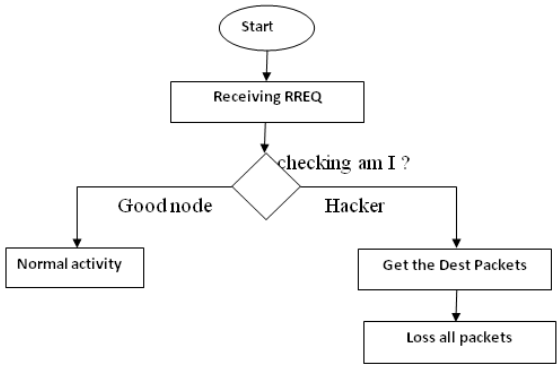

Fig4. Flow of Malicious activity

II. Related work:

During this [1] paper, author gift a completely unique Associate in Nursingonymous on demand routing theme for MANETs and determine variety of issues of antecedently projected works and propose an economical answer that has namelessness in an exceedingly stronger oppose model.

During this paper [2], author proposes a completely unique distributed routing protocol that guarantees security, namelessness and high dependableness of the established route in an exceedingly hostile setting, like impromptu wireless network, by encrypting routing packet header and abstaining from victimization unreliable intermediate node.

Pros and cons:

SDAR is Associate in nursing novel secure distributed anonymous routing protocol for Eduard MANET. Author mentioned the protocol and highlighted its main options that embody, (i) Non-source-based routing, (ii) versatile and reliable route choice, and (iii) Resilience against path hijacking. This SDAR use long public/private key pairs at every node for anonymous communication. These schemes area unit additional ascendible to network size, however need additional computation effort.

In during this [3] paper, author addresses some attention-grabbing problems arising in MANETs by coming up with Associate in Nursing anonymous routing framework (ALARM). It uses nodes current locations to construct a secure Eduard MANET map. Supported the present map, every node will decide that alternative nodes it desires to speak with. The ALARM framework is built that supports anonymous location-based routing in sure sorts of suspicious MANETS and it shows that that node privacy beneath this framework is preserved notwithstanding some of the nodes area unit stationary, or if the speed of movement isn\'t terribly high however it principally depends on cluster signature.

During this [4] paper, author proposes a completely purposeful identity-based encoding theme. The performance of the system is appreciating the performance of ElGamal encoding. The protection of the system is predicated on a natural analogue of the procedure Diffie-Hellman assumption. A cipher text security for identity-based systems is meant and projected a completely purposeful IBE system. The system has chosen cipher text security within the random oracle model forward BDH, a natural analogue of the procedure Diffie-Hellman drawback however the assailant have some negligible advantage in defeating the linguistics security of the system.

During this [5] paper, author presents Sybil Guard, a completely unique protocol for limiting the pervasive influences of Sybil attacks. Protocol is predicated on the Public network among user identities, wherever a grip between 2 identities indicates a human-established trust relationship. Sybil Guard, a completely unique protocol for limiting the pervasive influences of Sybil attacks is projected, that {is principally is especially is principally} used for reducing the Sybil attacks of the adversaries on the networks and to supply security to the network however it mainly depends on properties of the users.

Proposed system design:

In this paper, an approach has been proposed to combat black-hole attack in AODV routing protocol. In this approach any node uses number rules to inference about honesty of reply's sender.

Activities of a node in a very network show its honesty. To participate in information transfer method, a node should demonstrate its honesty. Early of simulation, all nodes area unit able to transfer data; so they need enough time to indicate its truth (Though each node are often a bearing less one). If a node is that the 1st receiver of a RREP packet, it forwards packets to supply and initiates judgment method on concerning replier. The judgment method is base on opinion of network nodes concerning replier.

The activities of node information are logged by its neighbors table given in fig.3. These neighbors area unit requested to send their opinion a couple of node. Once a node collects all opinions of neighbors, it decides if the replier may be a malicious node. The choice is base on range rules. The subsequent rules employed in this paper to gauge concerning honesty of a node in network. This judgment is base on nodes are activity in network

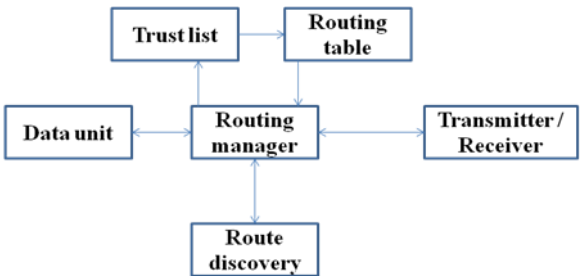

Fig.3 Combat Black Hole Attack Architecture

Applications:

- Civilian communications with MANET technology
- Large wireless Mobile ad-hoc network.
- Dynamic structured network

Modules

- Route discovery
  - Route-REQ
  - Route-REP
- Trust checking
  - Op-REQ
  - Op-REP
- Trust alert

Route discovery

- Route discovery is the process of finding route from source to destination.
- This process is done by making query by RREQ and getting Response by RREP

Trust checking

In our project, we are assuming each and every node having the trust list and also it has the trust value about neighbor nodes. Whenever source wants to make to route is

correct then its need to make OREQ and OREP (fig.5).

In real time trust list is updated by checking the activity of neighbor. If neighbor provides misbehavior then node updates with bad opinion.

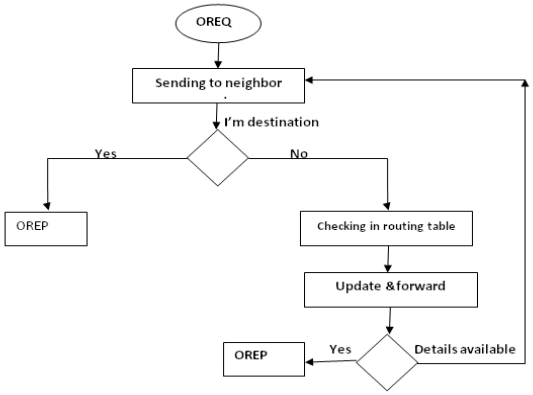

Fig.5 opinion packet sharing

Trust Alarm:

In this module, nodes can inform to other node about misbehaving activity others, however having thought on other node as malicious.

By this module, source node can avoid unnecessary delay in route discovery process

IV. Simulation model:

Simulations were conducted mistreatment the NS2 network simulator. Nodes within the network were organized to use 802.11 radios with an information measure of two Mbps and a nominal range of 250 m. so as to simulate most of the projected Byzantine attacks in NS2, the protocol freelance Byzantine attack simulation module was implemented. These modules provides the aptitude to simulate the region, Byzantine wormhole, and Byzantine overlay network hollow attacks without modifying the routing protocol

Fig.6 shows the results of malicious activity. Malicious node provides wrong information to source node.

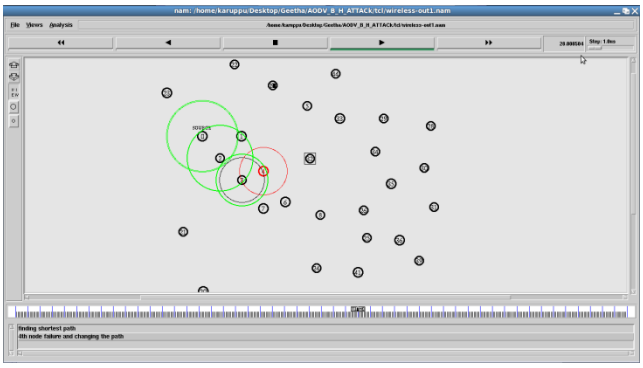

Fig.6 Malicious reply

Fig.7 shows the results of source activity. Source node makes opinion request to neighbor node.

Fig.8 shows the results of data transmission through correct path. And data securely transfer from source to destination.

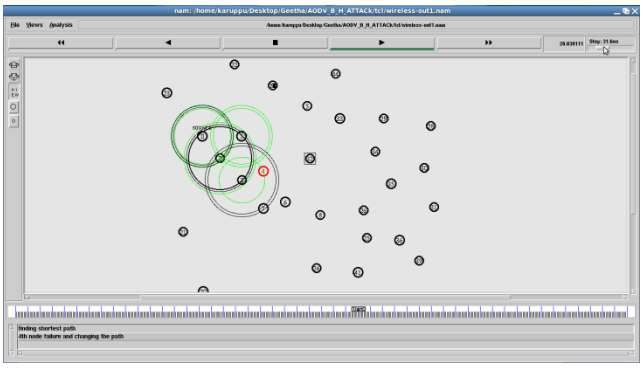

Fig.7 Opinion Packet sharing

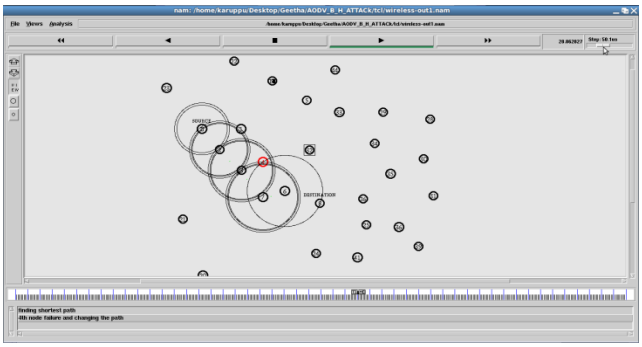

Fig.8 data transfer through other node

Fig.9 shows the comparison results of reply attack in Basic AODV, OP_AODV, MOP_AODV

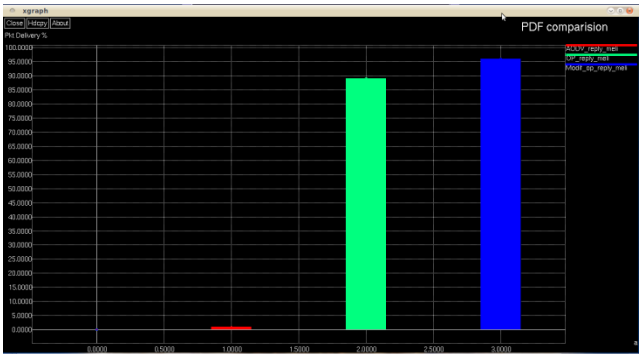

Fig.9 Pkt delivery in reply attack environment (Basic AODV, OP_AODV, MOP_AODV)

Fig.10 shows compression Pkt delivery in normal attack environment (Basic AODV, OP_AODV, MOP_AODV)

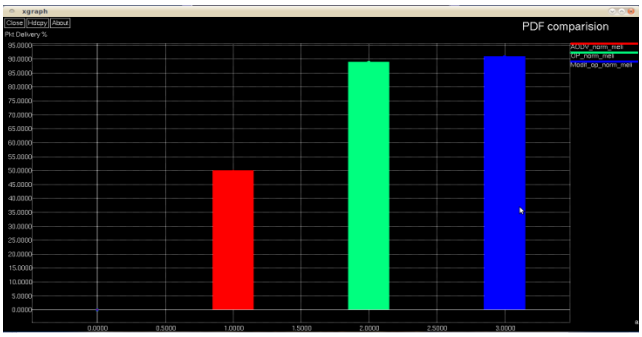

Fig.10 Pkt delivery in normal attack environment (Basic AODV, OP_AODV, MOP_AODV)

V. Conclusion:

It shows a clear and constant increase in the throughput because of the removal of Byzantine Faulty links. Similarly comparative graphs are drawn for delivery ratio. The simulated result shows an improvement over the existing scheme. This scheme is able to find out the faulty links within log n time where n is number of nodes of the path. The highly successful delivery of message with the ability to disperse and avoidance of faulty links is more secured and reliable than ordinary secured data transmission mechanism. Proposed scheme is effective in situations where reliability and security is most wanted in situations like MANET in military.

In this paper, due to less time duration we discussed only about removing misbehavior node but not discussed clearly about new node entry. So in our future work we will provide clear solution for new node entry.

ACKNOWLEDGMENT

We would prefer to acknowledge the efforts of ***Pantech ProEd Pvt ltd., India*** for guidance that helped us work flat out towards producing this research work.

REFERENCES

[1] "**On Flow Correlation Attacks and Countermeasures in combine Networks"**, Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei dynasty Zhao - 2004.

[2] "**Anonymous Communications in Mobile impromptu Networks**", Yanchao Zhang, Wei dynasty Liu and Wenjing Lou - 2005.

[3] "**Self-Organized Public-Key Management for Mobile impromptu Networks**", Srdjan Capkun, Levente sandwich 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 impromptu Networks**", Stefaan Seys and aristocrat Preneel - 2009.

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

[8] "**ALARM: Anonymous Location assisted Routing in Suspicious MANETs**", Karim El Defrawy and cistron Tsudik - 2011.

[9] "**Identity-Based secret writing from the Weil Pairing**", Dan Boneh, Matthew Franklin - 2001.

[10] "**SybilGuard: defensive Against sybil Attacks via Social Networks**", Haifeng Yu, archangel Kaminsky, Phillip B. Gibbons, patriarch Flaxman - 2006.

[11] "**Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms,"** *Commun. of the ACM*, vol. 4, no. 2, Feb. 1981.

[12] S. Capkun, L. Buttyan, and J. Hubaux, **"Self-organized public-key management for mobile ad hoc networks,"** *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

[13] J. Kong and X. Hong, "**ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks,"** in *Proc. ACM MOBIHOC', 03*, pp. 291–302.

[14] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "**Anonymous secure routing in mobile ad-hoc networks**," in *Proc. 2004 IEEE Conference on Local Computer Networks*, pp. 102–108.

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

[16] L. Song, L. Korba, and G. Yee, "**AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks,**" in *Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 33–42.

[17] "**ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks,**" Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, vol. 7, no. 8, pp. 1536–1550, 2009.

[18] 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.