International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

A Secure on Demand Routing Protocol

Tahseen Fatima[1], Prof. Sujata Mallapur[2]
[1]Student, Department of Computer Science and Engineering,
[2]Associate Professor& Head of Department
Godutai Engineering College for Women Kalaburgi, Karnataka, India

ABSTRACT
The flexibility and mobility of Mobile Ad hoc Networks (MANETs) have made them increasingly popular in a wide range of use cases. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. Both secure routing and communication security protocols must be implemented to provide full protection. The use of communication security protocols originally developed for wire line and Wi-Fi networks can also place a heavy burden on the limited network resources of a MANET. MA-NETs are dynamic, self-arranging, and foundation less gatherings of cell phones. They are normally made for a particular reason. Every gadget inside a MA-NET is known as a hub and must play the part of a customer and a switch. To address these issues, a novel secure framework is proposed. The framework is designed to allow existing network and routing protocols to perform their functions, whilst providing node authentication, access control, and communication security mechanisms.

Key Words: *Access control, node authentication, communication security mechanisms.*

1. INTRODUCTION
MOBILE autonomous networked systems have seen increased usage by the military and commercial sectors for tasks deemed too monotonous or hazardous for humans. An example of an autonomous networked system is the Unmanned Aerial Vehicle (UAV). These can be small-scale, networked platforms. Quadricopter swarms are a noteworthy example of such UAVs. Networked UAVs have particularly demanding communication requirements, as data exchange is vital for the on-going operation of the network. UAV swarms require regular network control communication, resulting in frequent route changes due to their mobility. This topology generation service is offered by a variety of Mobile Ad hoc Network (MANET) routing protocols. Communication across the network is achieved by forwarding packets to a destination node; when a direct source-destination link is unavailable intermediate nodes are used as routers. MANET communication is commonly wireless. Wireless communication can be trivially intercepted by any node in range of the transmitter. This can leave MANETs open to a range of attacks, such as the Sybil attack and route manipulation attacks that can compromise the integrity of the network. This is achieved by manipulating routing tables, injecting false route data or modifying routes. Man in the middle (MitM) attacks can be launched by manipulating routing data to pass traffic through malicious nodes . Secure routing protocols have been proposed to mitigate attacks against MANETs, but these do not extend protection to other data.

2. EXISTING SYSTEM
MANETs rely on intermediate nodes to route messages between distant nodes. Reactive protocols, such as Ad hoc On-demand Distance Vector (AODV), plan routes when messages need to be sent, polling nearby nodes in an attempt to find the shortest route to the destination node. Unsecured pro-active routing protocols exhibit vulnerability to packet replay and manipulation attacks. Due to a lack of source authentication, topology control messages can be broadcast frequently, which other nodes will treat as legitimate and use to update global topology

information. Optimized Link State Routing (OLSR) takes a proactive approach, periodically flooding the network to generate routing table entries that persist until the next update. The basic versions of AODV and OLSR lack security mechanisms, allowing malicious nodes to interfere with the network in a variety of ways.

DISADVANTAGES

- The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole (known as variants of black hole attacks).
- In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

3. PROPOSED SYSTEM:

Secure AODV (SAODV) is a security expansion of the AO-DV convention. SA-ODV directing message are carefully marked to ensure their honesty and genuineness. Subsequently, a hub that creates a directing communication cipher it through its confidential input, and the hubs that get this communication check the mark utilizing the sender's open key. The bounce tally can't be marked by the dispatcher, since it must be increased at each jump. Accordingly, to secure it an instrument in view of hash chains is utilized. In its essential shape, this makes it unthinkable for middle hubs to answer to RR-EQs in the event that they have a course towards the goal, on the grounds that the RREP message must be marked by the goal hub. To safeguard the joint effort component of AO-DV, SA-ODV incorporates a sort of assignment highlight that enables halfway hubs to answer to RR-EQ messages.

ADVANTAGES

- The security of the application is taken care where the nodes behavior is evaluated and malicious node is found out.
- The application makes the routing process very easy as the nodes which are good and holds true only be allowed to route the packets on the network.
- The energy consumption of the proposed system will be very less as only authenticated nodes are used for the transmitting the packets over the network.

4. SAODV ARCHITECTURE

This is interestingly with the methodologies proposed in past work, which center around securing particular communication based administrations. SUPERMAN is a structure that works at the system of the OSI display. It is intended to give a completely anchored correspondence structure for MANETs.

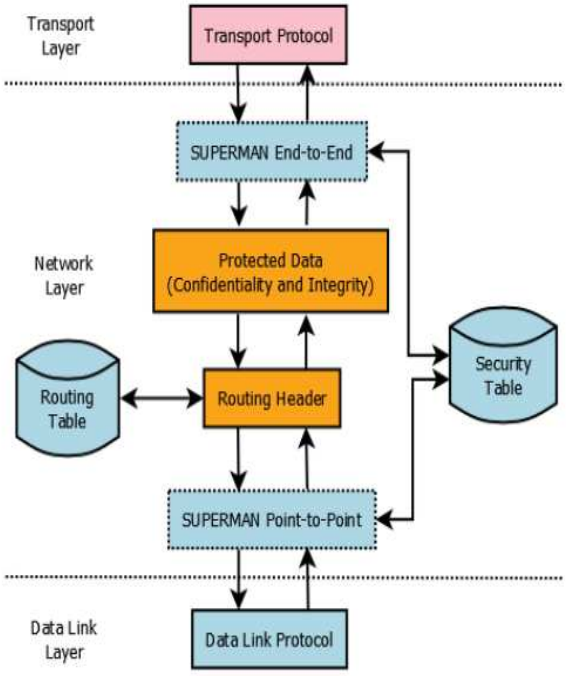

Figure 1: SAODV architecture.

The following security dimensions are recognized: Validation affirms the personality of conveying hubs. Confidentiality prevents unauthorized nodes from deriving meaning from captured packet payloads. And Communication security guarantees that data just streams amongst source and goal without being diverted or blocked and convey the substance to the planned beneficiaries. And finally Integrity checking enables hubs to contrast the present condition of information with a formerly recorded state so as to distinguish any progressions.

5. METHODOLOGY:

To break down secure AODV, the accompanying key zones were researched:

Initially knowing the idea of MANETS and Studying the outline of the conventions utilized. Further Implement the AODV convention utilizing the NS-2 test system. And Compare of security measurement scope for number of communication events required to secure communications between all nodes. Evaluate the convention AODV in correlation with the convention SAODV. Finally interpret the outcomes got.

6. SIMULATION

During the simulation of straightforward AO-DV, experimentation be approved more than 33 nodes. During NAM folder it will be able to exist simply analyze that the packet are falling or accomplishment to the target correctly or not. The following figure shows the animation captured during the simulation.

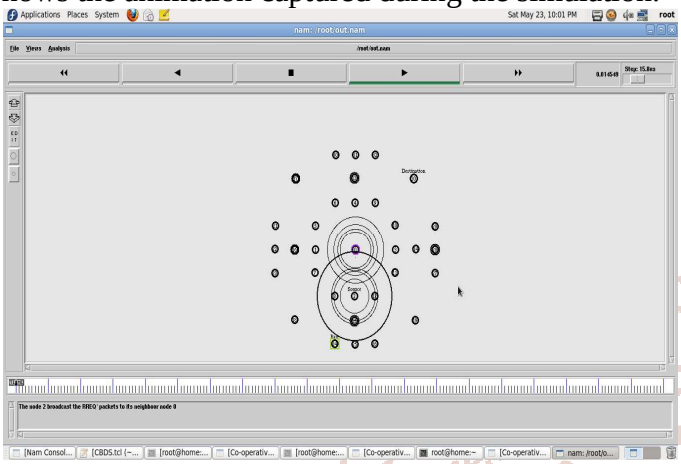

Figure 2: Results shows the Broadcast of Route REQuest from source nodes to neighbor nodes.

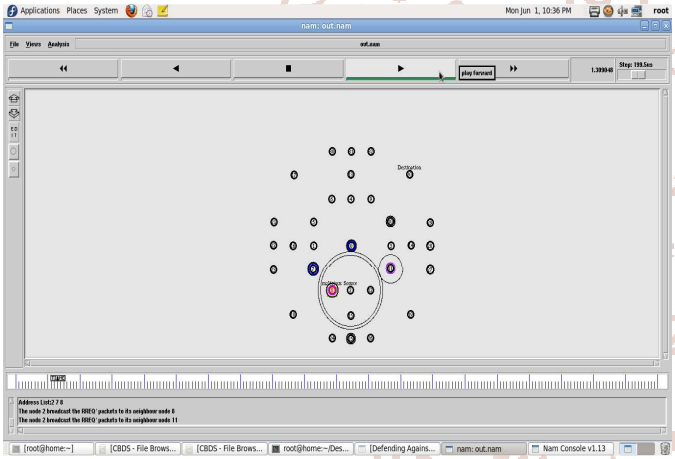

Figure 3: Result shows that the malicious nodes have been detected.

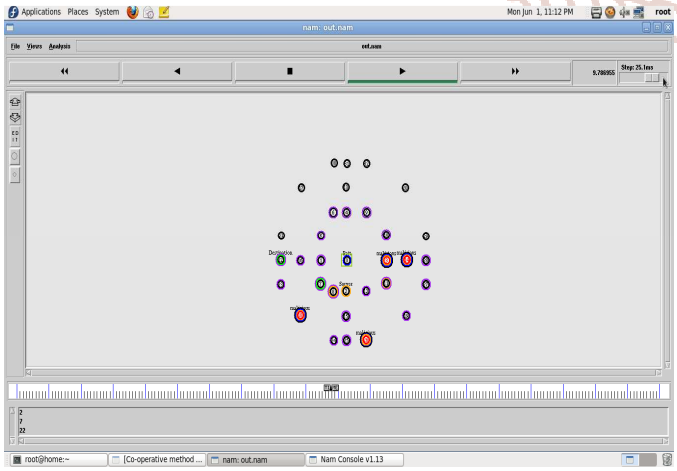

Figure 4: Results shows all spiteful nodules in the nets are perceived.

7. INTERPRETATION OF RESULTS:

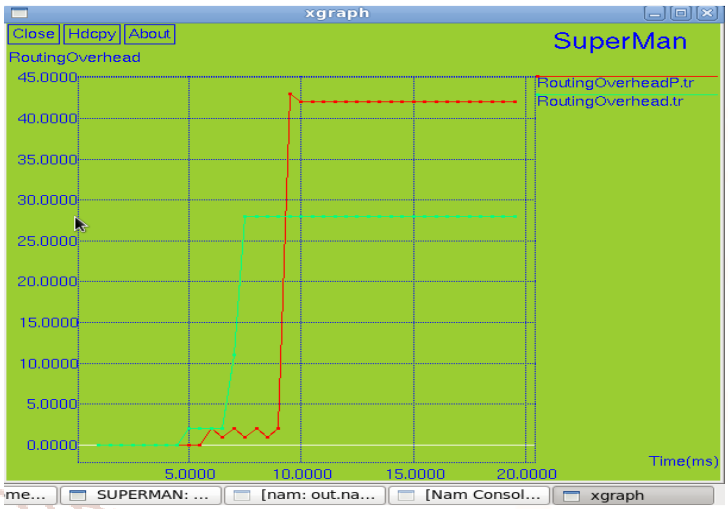

Figure 5: Results showing the Routing Overhead in comparison with AODV and SAODV

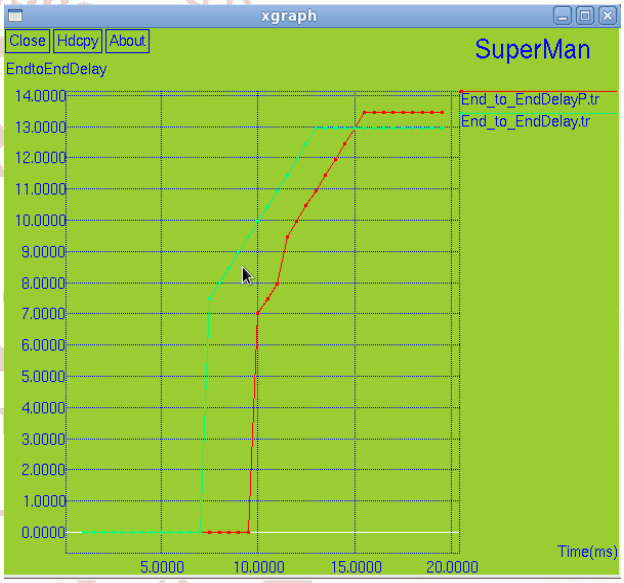

Figure 6: Results showing the End in the direction of End Delay in comparison with AODV and SAODV.

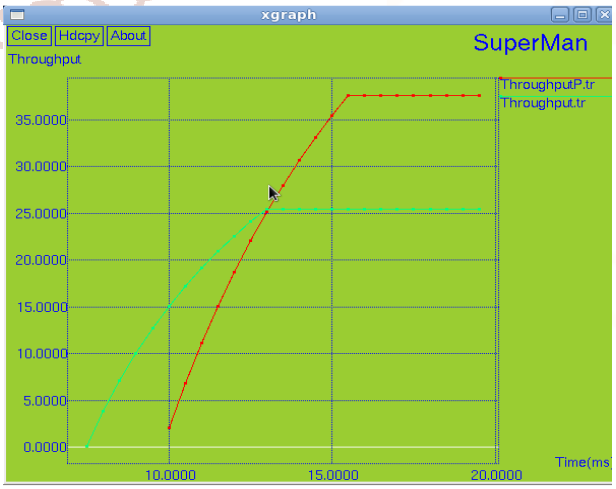

Figure7: Results showing the Throughput in comparison with AODV and SAODV

CONCLUSION:

Security using pre-existing routing protocol is a novel security system that ensures the system and correspondence in MANETs. Subsequently, it can be said to actualize a full suite of security administrations for self-ruling MANETs. It is expected to give a safe situation between two end-focuses paying little mind to course, and has been proposed by a few specialists to be a practical possibility for MANET security. Simulation has been undertaken and the results are reported and analyzed to determine the relative cost of security for SUPERMAN, compared between AODV and SAODV where relevant. This provides security to all data communicated over a MANET. It specifically targets the attributes of MANETs. It sacrifices adaptability to a range of networks, to ensure that MANET communication is protected completely and efficiently. A single efficient method protects routing and application data, ensuring that the MANET provides reliable, confidential and trustworthy communication to all legitimate nodes.

REFERENCES:

1. P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.
2. A. Chandra, “Ontology for manet security threats,” PROC. NCON, Krishnankoil, Tamil Nadu, pp. 171–17, 2005.
3. A. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.
4. P. C. Tsou, J. M. Chang, “A cooperative Bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture” 2014 22nd Euro micro International Conference on. IEEE, 2014, pp. 428–431.
5. D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks”, in Distributed Computing Systems Workshops, 2004. Proceedings.24th International Conference on. IEEE, 2004, pp. 698–703.
6. I. Rubin, A. Behzad, H. Luo and R. Zhang, “TBONE: A mobile backbone protocol for ad hoc wireless networks”, in proc. IEEE Aerosp. Conf, 2002, vol.6, pp.2727-2740.