A Novel method to Detect Black Hole attack in MANET using Efficient ACO Strategy for SEAD Protocol

Thamil selvi C.P,
HOD in Dept of Comp Science and Engineering,
Sasurie Academy of Engineering, Coimbatore.

ABSTRACT
It is highly essential to ensure security for data transmission. Number of such work is going on to ensure secure data transmission. Due to the high growth usage of mobile in this era, it is highly essential to make use of secure mechanism in mobile. Besides the advent growth of mobile there is also a parallel growth of threats. In order to provide better performance in the mobile architecture this work ensures security for mobile nodes. Every Mobile node is liable to attack. Such nodes were declared as malicious node. This work will provide efficient strategy to fight against threats like Black hole attack using the fitness function generated from ACO (Ant Colony Optimization).Further it stops the fake route display generated from the malicious node which further declared as malicious node. Extent of this work will be DDOS (Distributed Denial of Service) for transmission of packets between mobile nodes.

Keywords
AODV, SEAD Protocol, MANET's Threats, MANET Security.

1. INTRODUCTION
A Multi hop Mobile Ad hoc Network (MANET) is an infrastructure less in which mobile nodes communicate directly and cooperatively with each other. Each and every mobile node is highly distributed where it deals with Multicast technology. Since there is no proper access points or routers, and no configuration prior to setup of a MANET is required, it's very difficult to centralize administration on MANET where such set up make different issues such as routing, authentication, or congestion control. Also, due to high mobility, resource constrains (power, storage, and bandwidth) in MANET environment, and nodes operating in a dynamic topology, more challenges are encountered in routing.

The need of Ad-hoc On-Demand Distance Vector (AODV) routing protocol ensures the design principles of ADHOC mobile network. This protocol will be proactive when router is initiated. In enhance predefined routing table with entry destination and sequence number to figure out routing information. Further such incorporation leads to routing loop mechanism.

Another important feature of AODV protocol is time based node state maintenance. It ensures control packets like RREQ (routing request message) to communicate with other node for broadcasting message.

The need for IDS in MANET develops various security standards to make Mobile network reliable towards data transmission. The attack in MANET varies from general network attack and further classified based on the criteria. The classifications were listed as passive or active, internal or external, stealthy or non-stealthy. Black Hole attack is a kind of attack holds the above mentioned property. The node which makes such kind of attack was declared to be malicious and hence the attack known as Black Hole attack. A Malicious node absorbs all kind of packets and terminates further packet transmission. In other words, the network packets were further will not be send beyond malicious node. In this way, all packets in the network are dropped.

Deploying IDS in wireless sensor networks (WSNs) for mission critical applications (such as intruder detection and tracking) often face the fundamental challenge of meeting stringent spatial and temporal performance requirements imposed by users. For instance, a surveillance application may require any intruder to be detected with a high probability (e.g., >90%), a low false alarm rate (e.g., <1%), and within a bounded delay (e.g., 20 s).

2. RELATED WORK
This work focus on IDS in MANET based on Ground rules metrics. A survey proposed by Tiranch A. et al [1] in ad hoc networks classified IDS in two categories viz. Standalone and Cooperative. Standalone IDS are those in which IDS agent runs on each node independently whereas in Cooperative IDS, a monitor agent observes the behaviour of neighbouring nodes and learn accordingly. Loo et al [2] presented a standalone approach for detection in which intrusions are related to anomalies. An anomaly is declared when value of any feature exceeds threshold value. Yu and Xiao [3] proposed a decentralized approach to detect selective forwarding attack by changing the ACK packet format. Bhargav and Wang [4] had used features of both Standalone and Cooperative IDS to detect wormhole approach. ANDES [5] uses centralized concept to detect Black Hole, Sink Hole and Selective Forwarding attack by analyzing results of both data and management data. A lot of work has been done in this area, but none of the above mentioned approaches considered congestion of node as a case that can be misinterpreted with attacks. Moreover none of the researchers has thought of deploying ants for detection. The work [6] uses ants for load balancing that have memory and hence requires more energy for transmission. Researchers have applied the concept of Ants in finding optimal route in WSN and shows that ants can increase network lifetime as long as possible [7-11]. Dimple Juneja's [20] work gives the comparison study of various approaches.

Table1: Comparison with Existing Anomaly Detection Scheme

Schemes	Use of Intelligent agents	Cooperative/Standalone	Overheads	# of Attacks	Extensible
Loo et al.	No	Standalone	Computation, Storage(High)	3	Yes
Yu & Xiao	No	Standalone	Computation	1	No
Bhargava and Wang	No	Both	Computation, Storage(low), Communication	1	No
ANDES	Yes	Cooperative	Storage(low), Communication	6	Yes
EAR	Yes	Standalone	Storage(low), Communication(very low)	4	Yes

3. PROPOSED WORK

Two Secure MANET approaches like (1) Securing Ad hoc Routing and (2) Intrusion Detection [12] which was proposed in this work along with Description of Black Hole attack ACO and SEAD.

3.1 Secure Routing

The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [13] employs the use of hash chains to authenticate hop counts and sequence numbers in DSDV. Another secure routing protocol, Ariadne [14] assumes the existence of a shared secret key between two nodes based on DSR (reactive) routing protocol. The Authenticated Routing for Ad hoc networks (ARAN) is a standalone protocol that uses cryptographic public-key certificates in order to achieve the security goals [15]. Security-Aware Ad hoc Routing (SAR) uses security attributes such as trust values and relationships [16].

3.2 Intrusion Detection System

Zhang and Lee [17] present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly detection techniques. The use of anomaly based detection techniques results in too many number of false positives. Stamouli proposes architecture for Real-Time Intrusion Detection for Ad hoc Networks (RIDAN) [7]. The detection process relies on a state-based misuse detection system. Therefore, each node requires extra processing power and sensing capabilities.

3.3 Description of Black Hole attack

Security is the major issue in MANET. Majority of the attacks were against Physical, MAC and few more layers which deals with routing mechanism of Mobile ad hoc network. Primarily the attacks were classified based on the purpose (i.e) not forwarding the packets through routing mechanism, which affects sequence number and hop count. An attack would be described in such a way that the packets will be forwarded and further this stops the execution. The Black Hole attack malicious node waits for the neighbours to initiate a RREQ packet. Since the receivable RREQ Packet reaches the node, it will immediately send a false RREP packet with a modified higher sequence number. A malicious node where there is a possibility of Black hole attack which submerge all data packets of all objects and the packet will not be distributed further. The Figure 1 [18][19] describes Black hole attack in MANET

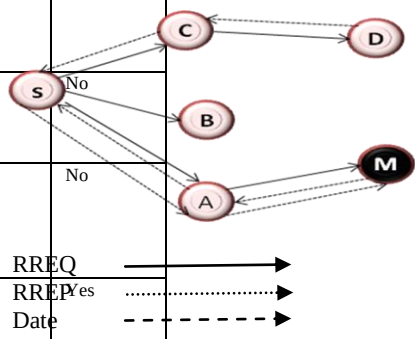


Figure 1: Black Hole Attack in MANET

3.4 ACO and SEAD

In order to avoid such a situation we have proposed a method for incorporating the ACO(Ant Colony Optimization) algorithm towards SEAD routing principles. The concepts of ACO describes the node characteristics and hence to make the node promiscuous.

In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. Our solution does an addition check to find whether the RREP_seq_no is higher than the threshold value. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbours. Here the threshold value is dynamically updated as in every time interval. This threshold value was given by ACO algorithm which will distinguish the nodes.

In SEAD routing protocol which will authenticate the nodes based on the hop counts and as well as the sequence number based on the threshold value generated by ACO. Since SEAD protocol deals with secret key sharing it the wise choice for implementing in MANET IDS.

4. HOW TO EVALUATE SEAD

In order to implement this, we have simulated using ns2 with 100 nodes where in previous study it was with 70 nodes. This table shows the simulation strategy implemented form MANET IDS.

Parameter	***Value***
Simulator	Ns-2(ver.2.33)
Simulation time	1000 s
Number of nodes	100
Routing Protocol	SEAD/AODV
Traffic Model	CBR
Pause time	2 (s)
Maximum mobility	60 m/s

No. of sources	5
Terrain area	800m x 800m
Transmission Range	250m
No. of malicious node	1

A new Routing Agent is added in ns-2 to include the black hole attack. In order to implement black hole attack, the malicious node generates a random number between 15 and 200, adds the number to the sequence number in RREQ and then generates the sequence number in RREP. In our simulation, the communication is started between source nodes to the Destination node in presence of the malicious node. The node number of source node, destination node and malicious node are 2, 7 and 0 respectively.
In the Figure 2 the nodes were numbered in sequence starting from right 1 to 7.

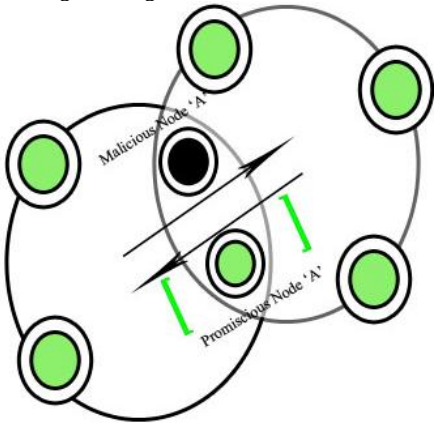


Figure 2: SEAD Protocol Implementation

4.1 EAR Network Model

Let G = (V, E) denote the network, V denotes set of all nodes in the network, n ε V denotes the number of nodes, and E denotes set of all links (i, j) where i, j ε V .For node i, link (i, j) exist if and only if j ε NBRi, where NBRi is the set of nodes that can be directly reached by nodei. The goal is to find the maximum number of attacks between Vs and Vd, where Vs, Vd ε V using minimum number of ants.

4.2 Ant Structures

The algorithm primarily employs two data structures i.e. Routing Table and Neighbour List which are explained as follows.
Routing Table: Routing table at each node stores the list of reachable nodes and their pheromone value. It is represented as structure consisting of following fields:

- ✓ Destination_id – This represents the address of the destination node
- ✓ Next_id – This represents the address of the previous node used to reach current node
- ✓ Ant_id – This represents a unique identifier used to represent each ant.
- ✓ Pheremone – This represents the value used by the node to calculate the probability of each adjacent node to be the next hop in order to reach the Destination.
- ✓ Protocol: SEAD.
- ✓ Age: Age of ant i.e. time taken by the ant to reach that node.
- ✓ Reliability: Ratio of packet sent and packet delivered by the node.

Neighbour list: Neighbour list is used to store the IDs and distance of all the neighbouring nodes as shown below

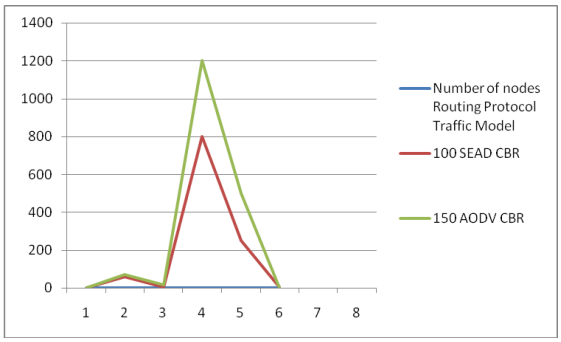
SOURCE ID	DEST_ID	ANT_ID	CT	TTL

Where CT stands for Creation time of ANT and TTL is Time to live for an ANT.

4.3 Algorithm Work Flow

Step 1: Activate a node with FA (Forward ANT)
Step 2: Choose the next Node (Neighbouring node)
Step 3: If Base Station launch BA (Backward ANT)
Step 4: Choose the next node
Step 5: Implement SEAD protocol (IDS Security)
Step 6: if source node STOP
Step 7: Proceed with the remaining nodes

5. RESULTS



This results show the comparision of SEAD and AODV protocol to detect the maximum number of malicious node. As the result the SEAD detect more number of malicous node than AODV. This experiment were done with 150 nodes to find maximum malicious node.

6. CONCLUSIONS & FUTURE WORK

MANET is an emerging technology but they are prone to security threats, routing attacks and intrusion. This paper presented an ant based novel approach reliability to detect anomalies. The proposed approach is decentralized, active and extensible. Simulation results show the efficiency of using ants for this purpose. In future detection of other types attacks using this algorithm may be attempted and more adaptive values for threshold can be explored.

Author Profile

Thamil selvi C.P, working as Head Of the Department of Computer Science and Engineering, Sasurie Academy of Engg, Coimbatore. She Received her B.E degree from Madurai Kamaraj University, Madurai 1993 and ME degree at Anna university of Technology, Trichy 2012 .She has nearly 9 years experience in academia and 9 years experience in industry.

7. REFERENCES

[1] A. tiranuch, and W. Jie ,“ A survey on Intrusion Detection in Mobile Ad hoc Networks”, Chapter 7, Wireless/Mobile Networks Security, Springer, 2006.

[2] Chong Eik Loo, Mun Young Ng, Christopher Leckie, Marimuthu Palaniswami. “Intrusion Detection for routing attacks in Sensor networks” International Journal of Distributed Sensor Networks, 2006.

[3] Bo Yu, Bin Xiao “Detecting Selective Forwarding Attacks in Wireless Sensor Networks” Greece: IPDPS, 2006 .

[4] Bharat Bhargav, Weichao Wang “Visualization of Wormholes in Sensor Networks. New York , NY, USA: ACM press , 2004.

[5] Sumit Gupta, “Anomaly Detection in Wireless Sensor Networks “, MS Thesis, University of Houstan.

[6] J. Bruten, O.Holland and R.Schoonderwoerd, “Ant-like agents for load balancing in telecommunications networks” Agents’97 Marina del Rey CA USA, 1997.

[7] Heng Chen, Depei Qian, Weiguo Wu, Lu Cheng, “Swarm Intelligence Based Energy Balance Routing for Wireless Sensor Networks” iita, Second International Symposium on Intelligent Information Technology Application., 2008

[8] L.Osadciw,R..Muraleedharan,“Jamming Attack Detection and countermeasures In Wireless Sensor Network Using Ant System” SPIE Defence and Security, Orlando, 2006.

[9] L.Osadciw ,R..Muraleedharan and, “Cross Layer Denial of Service Attacks in Wireless Sensor Network Using Swarm Intelligence” IEEE, 2006.

[10] L.Osadciw ,R..Muraleedharan,“ Decision Making in a Building access system Using Swarm intelligence and Posets” 38th Annual Conference on Information Sciences and Systems, Princeton University, 2004.

[11] Rajani Muraleedharan and Lisa Osadciw, “Sensor Communication Networks Using Swarm Intelligence”, IEEE Upstate New York.

[12] Ioanna Stamouli, “Real-time Intrusion Detection for Ad hoc Networks” Master’s thesis, University of Dublin, Septermber 2003.

[13] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks,” Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.

[14] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks,” Proc. 8th ACM Int’l. Conf. Mobile Computing and Networking (Mobicom’02), Atlanta, Georgia, September 2002, pp. 12-23.

[15] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, “A secure Routing Protocol for Ad hoc networks In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP’ 02), 2002

[16] S. Yi, P. Naldurg, and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks,” Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (Mobihoc’01), Long Beach, CA, October 2001, pp. 299-302.

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless adhoc networks," 6th annual international Mobile computing and networking Conference Proceedings, 2000.

[18] Payal N. Raj, Prashant B. Swadas, “DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST

BLACKHOLE ATTACK IN AODV BASED MANET” IJCSI International Journal of Computer Science Issues, vol. 2, 2009.

[19] Dokurer, Semih.”Simulation of Black hole attack in wireless Ad-hoc networks”. Master's thesis, AtılımUniversity, September 2006.

[20]. Dimple Juneja et al, “Design and Implementation of EAR Algorithm for Detecting Routing Attacks in WSN”, International Journal of Engineering Science and Technology Vol. 2(6), 2010, 1677-1683