Secured Energy Aware Routing For Increasing Network Lifetime Using AODV For WSN

Chandana M J
M.Tech, CiTech, Bangalore

Dr. Suresh.L
Principal, CiTech, Bangalore

Abstract: Mobile Ad hoc Networks (MANETs) are the emerging technology which have immense prospective to be engaged in decisive situations like for an instance war fields and profitable applications such as edifice, traffic inspection, habitat monitoring and smart homes and many other situations. Since various users use this technique concurrently over a solitary channel, security has become a main fear. Although there are several ways to safeguard a network and defend the network from several attacks, only if 100% security and maintain secrecy is a enormous dispute in latest trend. One of the chief challenge MANETs experience today is safety. Although the operation of sensor nodes in an antagonistic atmosphere makes the networks susceptible to a combination of possible attacks, the intrinsic energy and memory confines of sensor nodes makes usual safety solutions impracticable. The sensing expertise combined with dealing out with power and wireless communication makes it advantageous for being broken in big measure in upcoming years. The wireless communication technology also acquires a variety of safety fears. Herein discussing a wide range of attacks in WSN and their categorization mechanisms and different securities measures available to handle them including the challenges faced.

Keywords: Wireless Sensor Network; Security Goal ;Security Attacks; Defensive mechanisms; Challenges; Mobile ad hoc network (MANET), Black Hole, malicious node ,Gray Hole, Routing, AODV.

I. INTRODUCTION

WSN contents of thousand of low cost nodes which can either be fixed or arbitrarily deployed to supervise the environment. WSN is in tread for the past few years, and they deploy a huge number of small nodes. The nodes sense environmental change and account them to other nodes over flexible network. Sensor nodes are of great help for deploying in antagonistic environment or geographical areas.

Each node has a different sense, dealing, storage and communication units. The position is not predetermined and allows arbitrary deployment in remote terrains. Due to limitations in energy and range, sensors need to cooperatively work in multi-hop communication architecture and allows the communication of their sensed and gathered data to the adjacent base station. Contrasting wired networks where the material wires avoid an attacker from compromise the security of the networks, WSN face safety challenges.

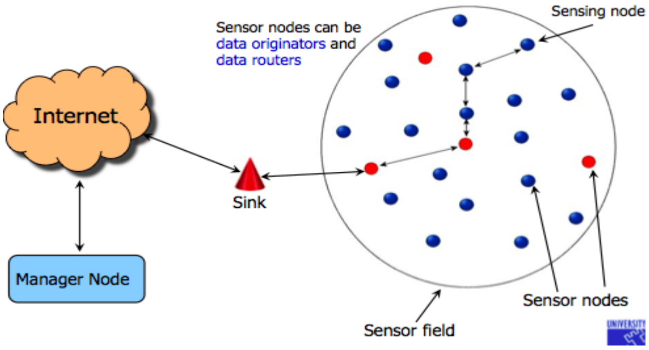

Figure 1

Basic components of WSN: (1) distributed sensors; (2) interconnect wireless networks; (3) a information gathering Sink also called as base station; (4) computing devices to analyze the received data.

AODV routing protocol is source initiated on demand routing protocol. AODV is prone to black hole attack. In [2], the authors have proposed that black hole nodes in a MANET work independently and proposed an algorithm to prevent a single black hole, but the proposed algorithm does not work in case of cooperative black hole attack.

II. PASSIVE ATTACKING

The observering the communicating channel by unofficial adversaries are generally termed as passive attacking. These attack is against confidentiality of messages.

A. ATTACK ON CONFIDENTIALITY

The major confidentiality problem in sensor network is not that they allow the gathering of data. Actually a large amount of data from the sensor node will be gathered and directed to the site of inspection. Relatively, sensor nodes increase the confidentiality issue since they have huge volumes of data which are easily offered through remote available. Some of the basic attacks against confidentiality are:

- ✓ *OBSERVE AND EAVESDROP:* This is the basic attack to confidentiality. By probing to the messages, the attackers can simply determine the communication messages.
- ✓ *ANALYZING THE TRAFFIC:* although data sent are encrypted, it still has the high probability of analyzing of the communication structure. Sensing behavior can highly disclose enough data to make an attacker to produce harmful effect in the network.

III. ACTIVE ATTACKING

The unofficial adversary observers and listens to manipulate the information stream in the transmission channel are generally called as active attackers. Namely

A. ATTACKING THE ROUTES IN WIRELESS NETWORKS

The attacks that happen in the network layer of the protocol stack are known as routing attacks. These include the following.

- ✓ Observing, changing and retransmitting of packets
- ✓ almost all the nodes act like a router or gateway
- ✓ Creating loops in the network
- ✓ Elongates routes
- ✓ Generates fake messages
- ✓ enhances end-to-end delay

B. SINKHOLE ATTACKING

Directing all the traffic to a single node is known sinkhole attacking. Through this attackers aim is to collect all the traffic to a particular node.

C. FORWARDING ONLY THE SELECTED PACKETS

An adversary node is made to drop certain packets which are very much efficient when combined with the attacks which collect data traffic.

D. MAKING THE NODE SYBIL

A malicious or adversary node clones and represents itself in a variety of locations and in this type of attacks malicious node acts with multiple identities in the network. Verification and various encryption methods can avoid an adversary from these attacks.

E. WORMHOLES ATTACKING

Through wormhole attacking, an adversary gathers all the packets from a node and tunnels them to some other node and again transmits back in the same network.

F. PHYSICAL ATTACKS

Sensor nodes mostly function in antagonistic surroundings, where it is highly susceptible physical tampering and damages or manipulate the programs or some malicious nodes can be placed in place of normal nodes.

G. DATA CORRUPTION

Modifying the information present in the data by an adversary gives up message privacy.

H. FAKE NODE

A fake node means, adversary can inject of malicious node and a user can put a node into the system which generates the fake messages or avoids the transfer of correct message.

I. NODE DUPLICATION ATTACKS

Abstractly, a node duplication attack is very easy; an adversary can add a malicious node to an accessible network by duplicating the nodes identity. A node duplicated like this can cause huge upset a sensor network in terms of performance.

J. PASSIVE DATA COLLECTING

An attacker using dominant sources can gather data from the sensor nodes if not encrypted. By probing the data that contents the information about the nodes where they are located easily allows an adversary to find the nodes and tamper them.

IV. SECURITY MECHANISM

The defense measures are essentially used to identify, avoid and recuperate from the different kinds of security attacks. Various schemes of security counter measures are been invented which can be arranged from higher to lower levels.

A. LOW-LEVEL MECHANISM

Primary security measures for secure wireless networks are,

✓ *ESTABLISHING KEY AND TRUST SETUP*

The basic prerequisite for building the sensor network is the founding of cryptographic keys. Since sensor nodes have limited power so public key cryptography is not suitable. Key-founding technique used should scale networks with hundreds and thousands of sensor nodes.

✓ *PRIVACY AND VALIDATION*

Almost all wireless network applications need security against eavesdrop, introduction and alteration of data packets. The end-to-end cryptographic techniques are required for a higher echelon of safety which needs keys be kept amid every closing stages points which are mismatched with submissive contribution and limited broadcasting.

✓ *SECRECY*

Herein the habitual networks, these Manets have also forced solitude concerns. At the start the these networks are located for legitimate purpose might subsequently be used in unanticipated ways.

✓ *SECURE PATHS*

Routing is a fundamental service for which makes communication in any networks possible. But, many present path finding protocols suffers various kinds safety issues. Like, an adversary may launch DoS to prevent transmission.

✓ *FLEXIBLE CAPTURING OF NODE*

In many applications, nodes are probably be positioned in places which are easily accessible by adversary. In such cases nodes can be easily captured, modified or relocated and also replaced with malicious nodes.

B. HIGHER-LEVEL SECURITY MEASURES

Higher-level measures for securing the sensor nodes, includes

✓ *SECURE GROUP SUPERVISION*

Every node in MANETS has small computing and communication capacities. But the data gathered are analyzed by groups of nodes. Therefore, secure protocols for grouping and managing is very much required.

✓ *INTERFERENCE RECOGNITION*

MANETs are vulnerable to various types of intrusion. MANETs needs a answer that is wholly dispersed and economical announcement, power and reminiscence supplies.

✓ *SECURE INFORMATION GATHERING*

The main advantage of a MANETs is the fine grain observing huge number of nodes. All the sensed data that should be gathered to prevent irresistible traffic on the base stations. For instance, the group of nodes might average the temperature of a particular area by combining the sensed values at various areas. Depending on the MANETs structure design gathering of data takes place in the network.

V. SIMULATIONS

All the experiments which are carried out for the working of proposed scheme are done with the help of network simulator ns-2. The 802.11 MAC layer implemented in ns-2 is used for simulation. An improved version of random waypoint model is used as the model of node mobility. The Performances of mainly three protocols have been examined: (i) Standard AODV protocol, (ii) AODV with the proposed algorithm, and (iii) AODV with two malicious nodes cooperating in a blackhole attack. The environment developed to carry out the tests uses five parameters: (i) PDR (ii) throughput (iii) energy (iv) Latency (v) Over head

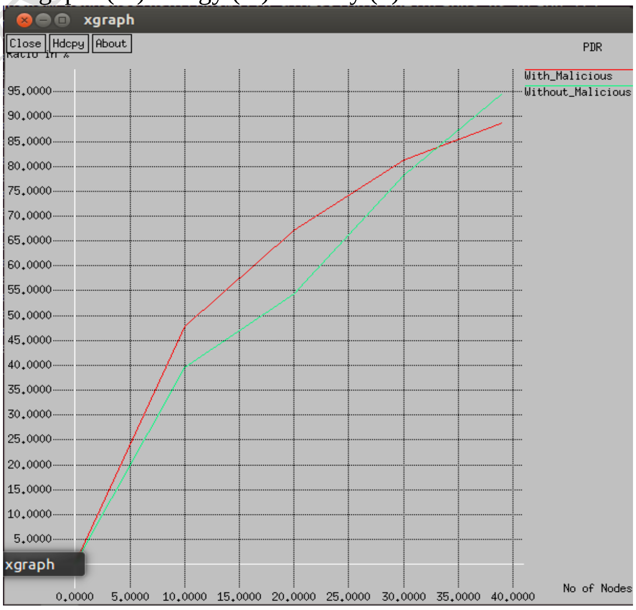

Figure 2: the graph showing the PDR in presence and absence of malicious node

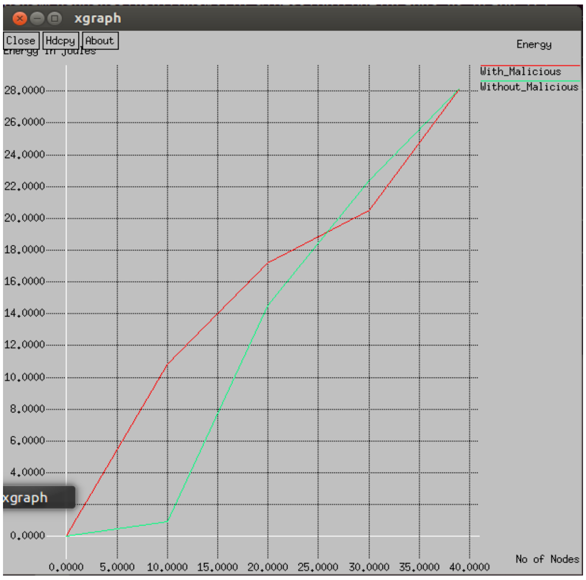

Figure 3: energy consumption graphs in the presence and absence of malicious node

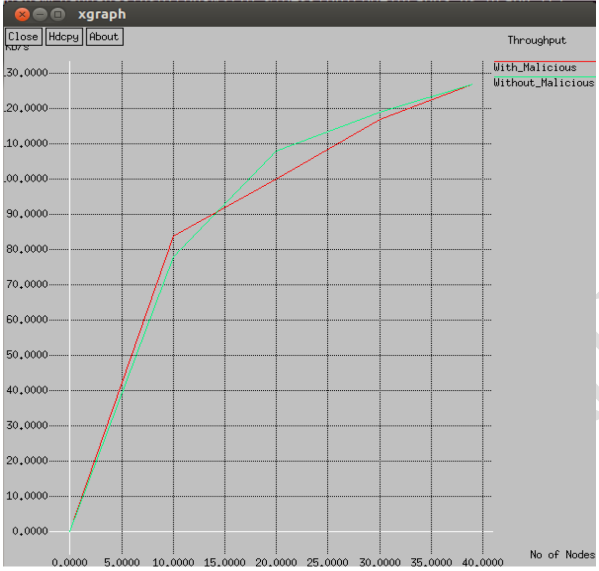

Figure 3: Graphs showing the throughput

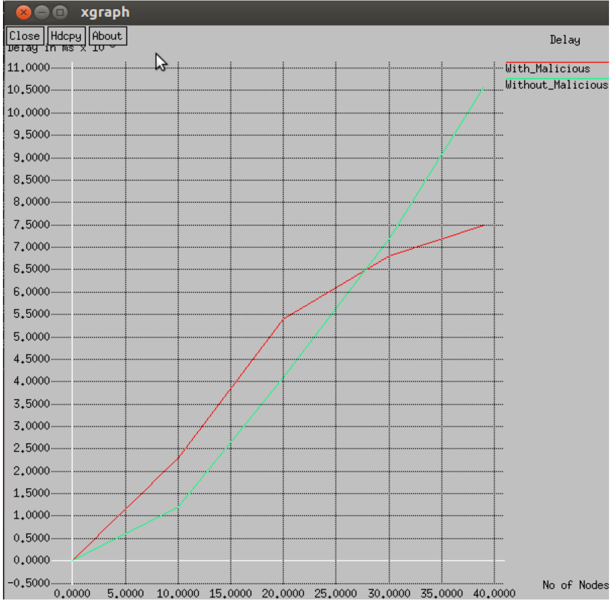

Figure 4: Graphs showing the delay

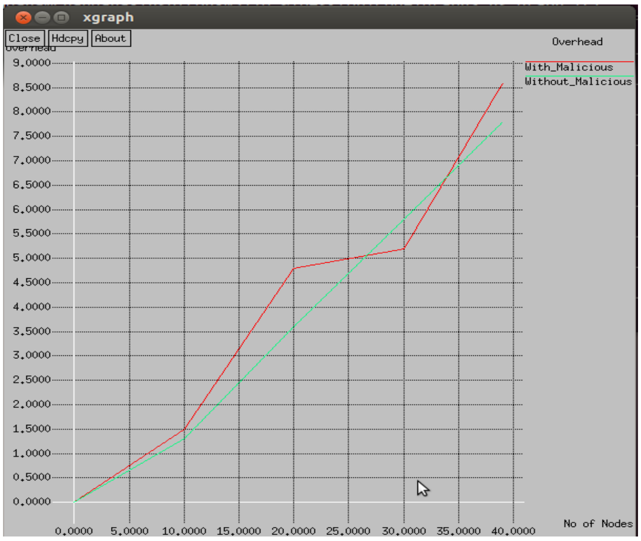

Figure 5: Graph showing the overhead in the network

VI. CONCLUSION

A new mechanism for examine the MANETs in presence of gray or collaborative black hole attacks. In this approach the source node selects stochastically an neighbor node with which it cooperate, malicious nodes are henceforth detected when there is a considerable drop in packet delivery ratio is noticed. As a future work 1) examine the feasibility of adjusting a new detecting mechanism to mitigate other type of collaborative attacks in MANETs 2)examine the integration of other detection mechanism with other popular message security methods in order to built a more comprehensive secure routing framework to protect MANETs against miscreants.

REFERENCES

[1] Perkins, E. Belding-Royer, and S. Das, “Ad-hoc on-demand distance vector (AODV) routing”, Internet Draft, RFC 3561, July 2003.

[2] H. Deng, H. Li, and D. Agrawal, “Routing security in wireless ad hoc networks”, IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.

[3] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks, In Proceedings of the 8th International Conference on Mobile Computing and Networking (Mobicm 2002), pp. 12-23, ACM, Atlanta, GA, Sept 2002.

[4] P. Papadimitratos and Z. Haas, “Secure routing for mobile ad hoc networks”, In SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan 2002.

[5] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, “A secure routing protocol for ad hoc networks”, In International Conference on Network Protocols (ICNP), Paris, France, Nov 2002.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing robust and ubiquitous security support for

mobile ad hoc networks", In International Conference on Network Protocols (ICNP), pp. 251-260, 2001.

[7] J.Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks", In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), 2001.

[8] F. Stajano and R. Anderson, "The resurrecting duckling", Lecture Notes in Computer Science, Springer-Verlag, 1999.

[9] S. Marti, T. Giuli, K.Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of MOBICOM 2000, pp. 255-265, 2000

[10] S. Buchegger and J. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation Of Nodes- Fairness In Dynamic Ad hoc NeTworks", In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, Jun 2002

[11] Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature", Vol.4, Issue 8, August 2014.

[12] T. Manikandan, S. Shitharth, C. Senthilkumar, C. Sebastinalbina, N. Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", Vol.3, Issue 3, March 2014.

[13] Jaspinder Kaur, Birinder Singh, "Detect and Isolate Black hole attack in MANET using AODV Protocol", Vol.3, Issue 2, February 2014, IJARCET.

[14] Bala Manju, Kaur Harjeet, SahniVarsha, " Study Of Black Hole Attack using different Routing Protocols in MANET ", Vol. 2, Issue 7 July, 2013.

[15] Latha Tamilselvan, Dr. V Sankaranarayanan,"Prevention of co-operative Black Hole Attack in MANET", Vol.3, No.5, May 2008.

[16] Marko Jahnke, Jens Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", IEEE Computer Society Washington, DC, USA, 2007.

[17] Semih Dokurer "Simulation of Black Hole attack in wireless Ad-hoc Networks" in September 2006.

[18] [18] Hidehisa Nakayama, "Detecting black hole attack on AODV based MANET by dynamic learning method".

[19] Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.

[20] Tamara Bonaci, Linda Bushnell and Radha Poovendran "Node Capture Attacks in Wireless Sensor Networks: A System Theoretic Approach".