ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Security Approach For Detection And Elimination Of Resource Depletion Attack In Wireless Sensor Network

Ambili M A[1], BijuBalakrishnan[2]

Department of Computer Science, Nehru Institute of Technology, Coimbatore[1, 2]

ABSTRACT: Wireless Sensor Networks came into prominence around the start of this millennium motivated by the omnipresentscenario ofsmall-sizedsensors withlimitedpower deployedinlargenumbers overan areato monitor different phenomenon.Theapplications ofWSNwererapidlyemerging& havebeen increasingly diverse,including medicalmonitoring, homeland security, industrialautomation, military application etc.. Thishighlightstheneedforsecurityassensornodesare highly susceptibletomanykindsofattacks.Someattackscalled resourceconsumptionattacksthatare difficultto detectwill deplete thenodes energyand thuspermanentlydisablethe network.Thesolemotivationforresearchin WSNhasbeen to providesecurityandto maximizethelifetimeofthenetwork, where network lifetimeis typically measuredfromtheinstantof deploymenttothe point whenone ofthe nodeshas expendedits limitedpowersource andbecomesin-operational–commonly referredas a firstnode failure. In thispaper, we considerhow routing protocols,affectfrom attackeventhosedesignedtobe secure, lack protection from these attacks, which we call Vampire attacks, which permanently disable networks by quicklydrainingnodes'battery power.These"Vampire"attacks are notspecific toanyspecific protocolwhich aredevastating, difficult todetect,andareeasy tocarryoutusingasfewasone malicioustinsidersending onlyprotocol compliantmessages.We proposean energyconstraintintrusiondetectiontechniqueto detecttheresource drainingattack.

KEYWORDS: Ad hoc networks, wireless networks, sensor networks, vampire attack, resource consumption attack, security.

I. INTRODUCTION

Wireless Sensor networks (WSN) have gained worldwide interest in these years. Advances in Microelectronic system and low power radio technologies have created low-cost, low- power, multifunctional sensor devices, which can sense, measure, and collect information from the environment and transmit the sensed data to the data by a transceiver. Sensor nodes can use battery as a main power source and harvest power from the environment like solar panels as a secondary power supply. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Simplicity in WSN with resource constrained nodes makes them very much vulnerable to variety of attacks.

A great deal of research has been done to enhance survivability [2] [5] [10] [11] on wireless ad hoc sensor networks. While these schemes can prevent attacks on the short term availability of a network, they do not address attacks that affect long-term availability—the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Thus, in this paper, we consider the routing protocol. Although they are designed to be secure, lack protection from vampire attacks [1].

The remainder of this paper is organized as three sections. The first section gives an idea of what is resource depletion attack and how it will drain the battery power of nodes. The second section explain the related work which familiarizes the earlier security measures on wireless sensor network. After that, the proposed energy constraint intrusion detection system is explained and lastly we conclude our paper.

RESOURCE DEPLETION ATTACKS

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. This attack is not specific to any protocol. Few kinds of attacks are carousal and stretch attack.

CAROUSAL ATTACK

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. An example of this type of route is in Fig. 1 the thick path shows the honest path and thin shows the malicious path.

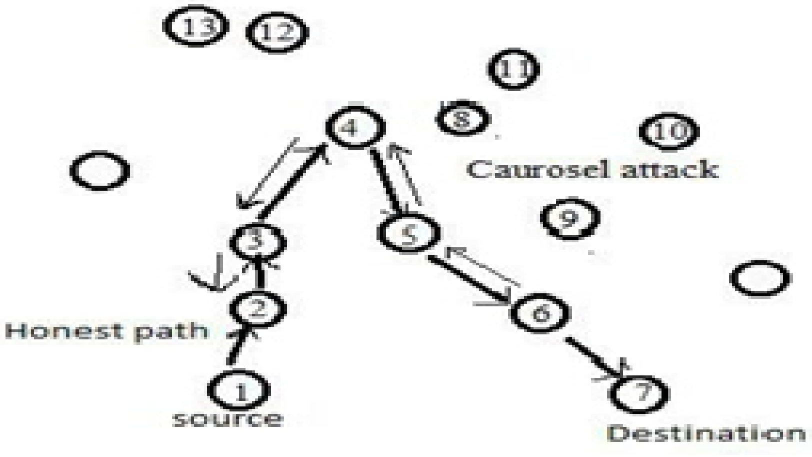

Fig. 1. Shows the carousel attack same node appears in the route many times

STRETCH ATTACK

Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. In the example given below honest path shown with thick lines and adversary or malicious path with thin lines.The honest path is very less distant but the malicious path is very long to make more energy consumption.

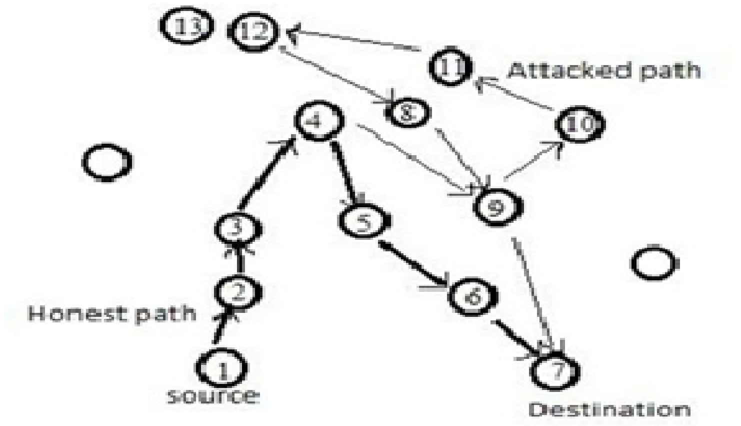

Fig .2 Shows Stretch attack with two different paths from source to destination.(4-9-10-11-12-8-9—long route).

Per-node energy usage under both attacks and without any attack is shown in Fig. 3. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10 percent of their total energy reserve per message.

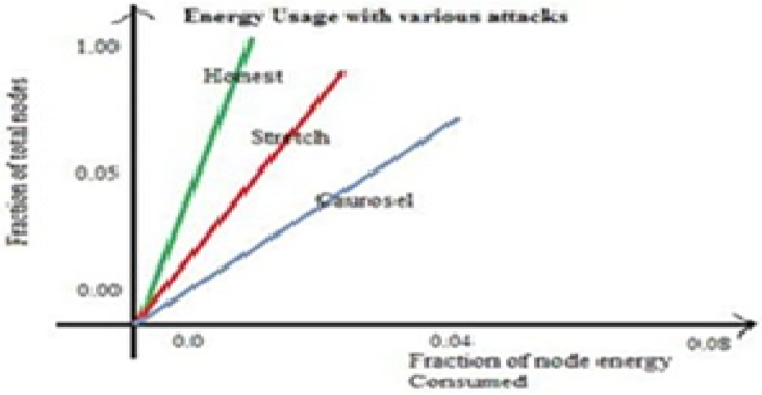

Fig.3. Node energy distribution under various attack scenarios

II. RELATED WORKS

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

The problem of security has received considerable attention by researchers in ad hoc networks. Vulnerabilities in WSN could occur based on certain dimensions in accordance with the characteristics of dynamic topology and lack of central base station. Many schemes proposed in the literature deal with the detection and /or prevention from resource exhaustion attack mostly confined to other levels of protocol stack eg.,Medium Access Control layer(MAC) and application layer. There exist only little discussion and no through analysis of resource draining attack in routing layer. Some of the previous works are:

1. Vampire Attack: Draining Life From Wireless Ad Hoc Sensor Network: This explores resource depletion attack in routing protocol layer, which permanently disable the network. In this a new protocol called PLGP is used for routing the packet.

2. Provably secure on demand source routing in Mobile Ad hoc Networks:Systematic way of analysis for flows in ad hoc routing protocol is advocated security is precisely defined, and routing protocols for mobile ad hoc network is analyzed rigorously.

3. INSENS: Intrusion Tolerant Routing In Wireless Sensor Network:INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and base station. INSENS does not rely on detecting intrusions; but rather tolerate intrusion by bypassing the malicious node.

4. SNEP Protocol:SNEP SNEP protocol was designed as basic component of another protocolSPINS (Security protocol was designed as protocol for wireless Sensor Networks) that was basically designed for secure key distribution in wireless sensor networks. SNEP define the primitives for authentication of sensor node, data confidentiality and data integrity. However the drawback of this protocol is lower data freshness. SNEP protocol uses shared counter for semantic confidentiality not initial vectors. Using SNEP the plain text is ciphered with CTR encryption algorithm. Both sender and receivers are responsible to update the shared counter once when they sent or receive cipher blocks. Therefore sending counter in message is not important, however every message has message authentication code (MAC). This is computed from cipher data with the help of CBC-MAC algorithm. When the receiver node receives data it recomputed MAC and compared with the received MAC.

ENERGY CONSTRAINED INTRUSION DETECTION SYSTEM

I propose an energy constrained intrusion detection system along with clean state secure routing protocol as ad hoc routing protocol. In this the packets are transmitted between source and destination through the intermediate nodes using ad hoc routing protocol PLGP [6] . A backtracking technique will prevent the packet moving away from destination. Thus it resist vampire attack. In addition to this energy level of nodes is compared to identify the malicious node. Thus malicious node is detected and eliminated from network by notifying to other node about the detection.

Clean State Secure Routing Protocol

The PLGP protocol is modified as clean state secure routing protocol such that they can resist vampire attacks during the forwarding. PLGP was vulnerable to vampire attacks even though they were said to be secured. When the route discovery begins each node has a limited view about the network. As already said nodes discover the other nodes in a group by broadcasting a certificate id, signed by the public key of the online authority, thus forming a single group and a tree structure that will be used for addressing and routing. All nodescompute the same address as the other nodes they also learn each other's virtual address as well as their cryptographic keys. The final address is verifiable after the network convergence and all forwarding decisions can be independently verified.

Topology Discovery- Tree Formation And Route Discovery

Trees are formed as nodes form group. Each node starts with group size 1 and virtual address 0 so that one group is formed. Similarly other groups are also formed. When two nodes form a group their group size becomes 2 with one node taking a virtual address 0 and other taking the address 1.Each group can have their own group address. Example: node 0 in one group0 becomes 0.0 and node 0 in group 1 becomes 1.0. Each time a group is added or merged the address of each node is lengthened by one bit .Thus a tree structure is formed with address in the network and node address as leaves. Nodes announce its presence by broadcasting a Id, public key signed by online authority. Generally small groups form with 1 node later they merge to form large groups. For example when two groups merge to form a large group they broadcast their group id to each other and precede with the merge protocols. Groups generally stay within the radio range incase if they have grown large they communicate through gateway nodes.

Each node stores the id of one or more nodes such that they can know that the other group exists such that every node within a group will end up with the next-hop path to every other group as in distance vector. Thus a tree is formed and the route is chosen in this manner until all network nodes are members of single group. By the end of this phase each node will know the virtual address, public key, certificate because they do communicate and broadcast.

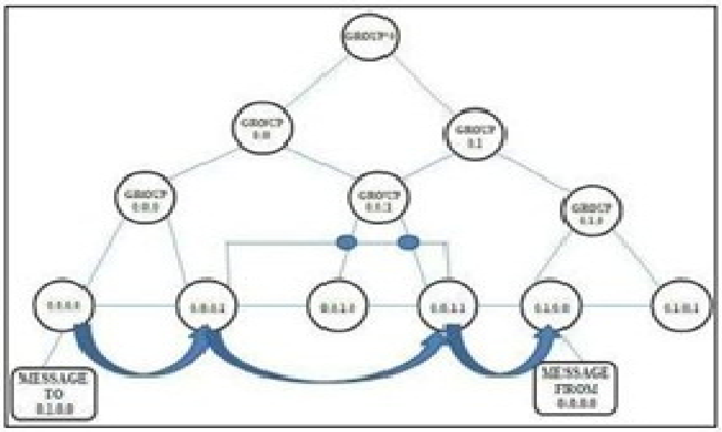

Fig: 4.Group identification

Forwarding of Packets

During this phase each node is independent of other node and hence the decision made by them is also independent. When a node receives a packet it determines the next hop by finding the most significant bit(MSB) address as it differs from the messages originators address(see Figure 4) as it differs from the originators address. When a packet is moving within a group and when they want to move to the next group they shortens the logical distance to destination since their address must be close to the destination.

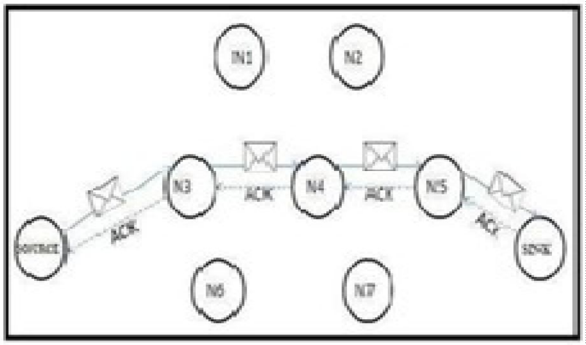

Fig 5: Packet Forwarding

Path Tracking Technique

In this a verifiable path history is added to packet, similar to route authentications in Ariadne [7] and path-vector signatures in [13]. Each node uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, it this by attaching a nonreplayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never traveled away from its destination in the logical address space.

Energy Constraint IDS

The intrusion detection system is to detect the presence of malicious node in the network. Each node in the network will have certain energy. The packets are forwarded with the expense of the energy of the node. The energy level of malicious node will be twice/thrice of that of legitimate nodes. Thus by comparing the energy level of node the malicious node can be detected and thus eliminated

III. CONCLUSION

In this paper, we define Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. An energy constraint intrusion detection scheme is introduced along with clean state secure routing protocol

REFERENCES

[1] Eugene Y. Vasserman , Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011

[2] ImadAad, Jean-Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004.

[3] GergelyAcs, LeventeButtyan, and IstvanVajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on mobile computing 05(2006),no.11.

[4] H. Chan and A. Perrig, "Security and Privacy inSensor Networks," computer, vol. 36, no. 10, pp.103-105, Oct. 2003.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion- Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29,no. 2, pp. 216-230, 2006.

[6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[7] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.

[8] M.G. Zapata and N. Asokan, "Securing Ad Hoc RoutingProtocols," Proc.First ACM Workshop Wireless Security (WiSE), 2002.

[9] R.C. Shah and J.M. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," Proc. IEEE Wireless Comm. And Network Conf. (WCNC), 2002.

[10] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug.2004

[11] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.

[12] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54- 62, Oct. 2002.

[13] L. Subramanian, R.H. Katz, V. Roth, S. Shenker, and I. Stoica, "Reliable Broadcast in Unknown Fixed- Identity Networks," Proc. Ann. ACM SIGACT- SIGOPS Symp.Principles of Distributed Computing, 2005.