IJIRSET

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st&22ndMarch Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Provably Secure Routing and Defending Against Vampire Attacks in Wireless Ad Hoc Sensor Networks

R. Sangeetha, R.Deepa, C.Balasubramanian

PG Scholar, Dept of Computer Science and Engineering, P. S. R. Rengasamy College of Engineering for women, Sivakasi, India

Assistant Professor, Dept of Computer Science and Engineering, P. S. R. Rengasamy College of Engineering for women, Sivakasi, India

Head of Department, Dept of Computer Science and Engineering, P. S. R. Rengasamy College of Engineering for women, Sivakasi, India

***Abstract*:** Wireless ad hoc sensor network focus on the conservation of the energy available at each sensor node. Vampire attacks are not explicit to any particular protocol, but rather rely on the properties of many popular classes of routing protocols. A distinct vampire can shrink network large energy usage on whole network. Find that all examined protocols are vulnerable to Vampire attacks, which are destructive, not easy to intellect, and are easy to carry out using as few as one malicious insider sending only protocol yielding messages and moderate these types of attacks including a new concept of protocol that provably bounds the damage caused by vampires during the packet forwarding phase. The empirical result shows that, the graph analysis of Clean Slate Routing Protocol and Modified Clean Slate Routing Protocol, finally the result concludes that Modified Clean Slate Sensor Routing Protocol achieves greater power than the Clean Slate Routing Protocol.

Keywords— Denial of service, security, routing, ad-hoc networks, sensor networks, wireless networks.

I.INTRODUCTION

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Sensors are spread in an environment without any predetermined infrastructure and cooperate to execute common monitoring tasks which usually consist in sensing environmental data from the surrounding environment.

Wireless sensor networks provide unique opportunities of interaction between computer systems and their environment. Their deployment can be described at high level as follows: The sensor nodes measure environmental characteristics which are then processed in order to detect events. Upon event detection, some actions are triggered. This very general description applies to extremely security critical military applications as well as to such kind ones.

One of the main design issues for a sensor network is conservation of the energy available at each sensor node. The energy efficiency of a node is defined as the ratio of the amount of data delivered by the node to the total energy expended. Higher energy efficiency implies that a greater number of packets can be transmitted by the node with a given amount of energy reserve.

II.DENIAL OF SERVICE ATTACK

Adversary injecting malicious information or altering legitimate routing setup messages, or can prevent the routing protocol from functioning correctly. For example, an attacker can forge messages to convince legitimate nodes to route packets in a way from the correct destination.
Vampire attack is one of the resource depletion attacks. The resource depletion attack focuses the node's batteries life. Vampire attacks affect any protocol and utilize the properties of routing protocols classes such as source routing, distance vector and link state and geographic and beacon routing.

Dynamic Source Routing (DSR) Protocol is a stateless protocol do not store or maintain any routing information at the nodes. The source node specifies the entire route to a destination within the packet header, so intermediaries do not make independent forwarding decisions, relying rather on a route specified by the source. An adversary arranges packets with knowingly establish routing loops sends packets in circles targets source routing protocols by take advantage of the limited verification of message headers at forwarding nodes, allowing a single packet to repetitively traverse the same set of nodes that is called Carousel attack. In stretch attack, an adversary develops the long route between the source and destination. Both attacks perform on stateless protocol.

Stateful protocol store and maintain the routing information at the nodes. In Directional antenna attack, an adversary have modest control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy by restarting a packet in various parts of the network. In the malicious discovery attack, the adversaries induce a supposed topology. Both attacks perform on stateful protocol such as Optimized Link State Routing Protocol (link state) and Destination-Sequenced Distance Vector (DSDV).

III.RELATED WORK

David R.Raymond, Randy C.Marchany, Michael I. Brownfield and Scott F.Midkiff, discussed denial-of-sleep attack, in which a sensor node's power supply is targeted. Attacks of this type can reduce the sensor lifetime from years to days and have a disturbing impact on a sensor network. This paper proposed three contributions for sensor network security.

First, it classifies denial-of-sleep attacks on WSN MAC protocols based on an attacker's knowledge of the MAC protocol and ability to penetrate the network. Second, it explores potential attacks from each attack classification, both modeling their impacts on sensor networks running four leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks on three of the protocols. Finally, it proposed a framework for defending against denial- of-sleep attacks and provides specific techniques that can be used against each denial-of-sleep vulnerability.

Bryan Parno, Mark Luk, Evan Gaustad and Adrian Perring have introduced a new secure routing protocol for sensor networks. Our protocol requires no special hardware and provides message delivery even in an environment with active adversaries. Design a new sensor network routing protocol with security and efficient yet highly resilient to active attacks our protocol assigns a network address to each node and establishes routing tables using a recursive grouping algorithm.

For a given topology, the algorithm proceeds entirely deterministically, preventing attacks on routing information and limiting a subverted node's ability to perform malicious actions. The existing secure routing protocols introduced either an unacceptable level of complexity or an excessive performance penalty.

Jing Deng, Richard Han, Shivakant Mishra, had proposed an Intrusion tolerant routing protocol for wireless sensor networks (INSENS). INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station. The scope of damage inflicted by intruders is further limited by restricting flooding to the base station and by having the base station order its packets using one-way sequence numbers.

Jing Deng, Richard Han and Shivakant Mishra, have discussed Denial of service (DoS) attacks can cause severe damage in resource constrained, wireless sensor networks. In WSNs, an adversary can launch with little effort a path-based denial of service (PDoS) attack that will have a severe widespread effect on the WSN, disabling nodes on all branches downstream of the path, due to the tree-structured topology of WSNs. To defend against a PDoS attack, an intermediate node must be able to detect spurious packets or replayed packets, and then reject them.

Rahul C.Shah and Jan M.Rabaey have discussed sensor networks has led to a number of routing schemes that use the limited resources available at sensor nodes more efficiently. These schemes typically try to find the minimum energy path to optimize energy usage at a node. In this paper addressed lowest energy paths may not be optimal from the point of view of network lifetime and long term connectivity.

To optimize these measures, proposed a new scheme called energy aware routing that uses sub optimal paths occasionally to provide substantial gains. This paper proposed new protocol named energy aware routing. This protocol to increase the survivability of networks, it may be necessary to use sub-optimal paths occasionally.

To achieve this, multiple paths are found between source and destinations, and each path is assigned a probability of being chosen, depending on the energy metric. Every time data is to be sent from the source to destination, one of the paths is randomly chosen depending on the probabilities. Also different paths make an effort continuously, improving tolerance to nodes moving around the network. Using probabilistic forwarding to send traffic on different routes provides an easy way to use multiple paths without adding much complexity or state at a node.

IV.SYSTEM MODEL

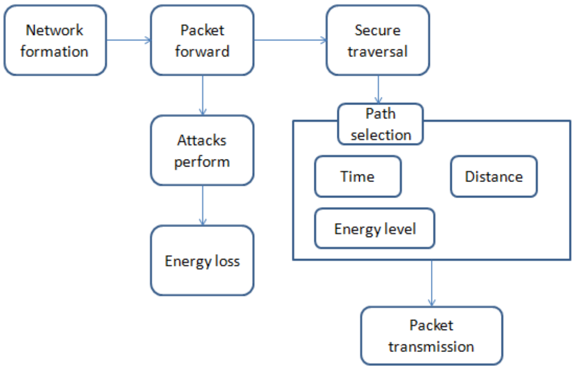


Fig 1: System Model

In the block diagram describes the system model, first create network formation with wireless nodes in which each node has the initial energy value. An adversary perform the attacks during the packet forwarding, this causes the loss of energy in wireless networks. Using thesecure packet traversalalgorithm, to protect malicious action and achieving the node's battery life.

The major components of the system architecture are network formation, attacks on protocol, security against vampire attacks.The various systems are briefed below:

A.NETWORK FORMATION

A network describes a collection of nodes and the links between them. Source node wish send the packet to destination through intermediate nodes. Packet contains the control information and user data. Network creation is the process of create the N number of nodes within the network. Each and every node has node id and initial energy value by its creation time. The nodes are wished to transfer the data in one node to another. Select the source and destination node and also maintain the neighbor list.

B.ATTACKS ON PROTOCOL

Resource depletion attacks focus on sinking the quantity of resources used by nodes like battery power, storage, memory etc, thus reducing the overall capacity of the network. Existing schemes can prevent attacks on the short term availability of a network, but do not address attacks that affect long-term availability. The most permanent denial of service attack is to entirely deplete node's batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest.

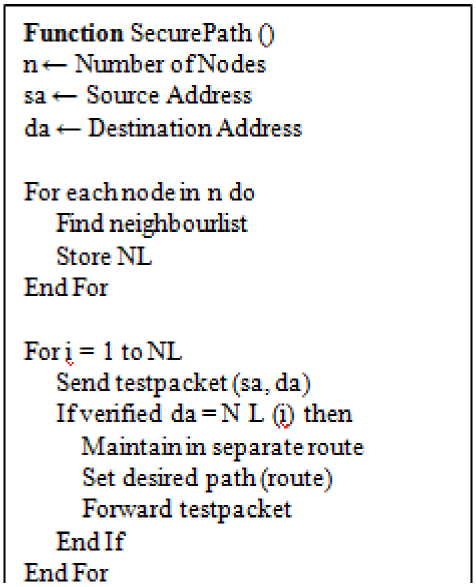
During the forwarding phase the clean slate sensor routing protocol is used (PLGP). All decisions are made independently by each node. Forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks.

C.SECURE PACKET TRAVERSAL

PLGP refers clean-slate secure sensor network routing protocol by Parno, Luk, Gaustad, and Perrig. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current. Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network, the node knows only itself.

Nodes discover their neighbors using local broadcast, and form ever expanding neighborhoods stopping when the entire network is a single group. All over this process, nodes build a tree of neighbor relationships and group membership that will later be used for addressing and routing. At the end of discovery, each node should compute the same address tree as other nodes.

The original version of the protocol is vulnerable to Vampire attacks. PLGP with attestations (PLGPa) 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 and also achieve the highest battery life in order to avoid the avoid the unconditional overhearing.



```
Function SecurePath ()
n ← Number of Nodes
sa ← Source Address
da ← Destination Address

For each node in n do
    Find neighbourlist
    Store NL
End For

For i = 1 to NL
    Send testpacket (sa, da)
    If verified da = N L (i) then
       Maintain in separate route
       Set desired path (route)
       Forward testpacket
    End If
End For
```

Secure Packet Traversal

Power consumption for data delivery depends on the three factors such as distance, time, and packet size. To find the distance between the nodes and transmission time is the amount of time from the beginning until the end of a message transmission.

D.EXPERIMENTAL RESULTS

The figure 5.16 shows the analysis result of energy retain on the nodes with respect to number of nodes. modified sensor routing protocol save the energy as much as greater than clean slate sensor routing protocol during the data transmission.

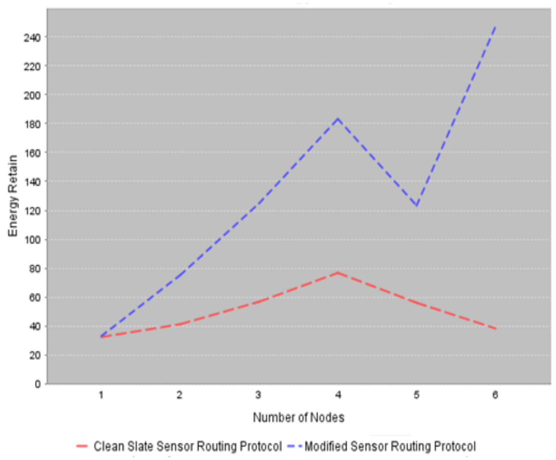


Fig 2: Energy Consumption

V.CONCLUSION AND FUTURE WORK

In this work, vampire attacks are defined and new approach against the vampire attack is implemented to achieve the increased power consumption by the effective nodes. The packet forwarding algorithm goes secure forwarding of packet to destination posture of the node. It captures the transfer message packet from nodes which want to send the data and it retrieves the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list which has high performance from existing evaluation. If this next hop is present in the neighbor list it simple transfer packet to next hop otherwise it simple delete the packet from its network. Future work aims at extending their work to provide authentication to data transfer.

REFERENCES

[1] Eugene Y.Vasserman and Nicholas Hopper, “Vampire attacks: Draining life from wireless ad-hoc sensor networks” (2013).

[2] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, “Effects of denial-of-sleep attacks on wireless sensor network MAC protocols”(2009).

[3] David R. Raymond and Scott F.Midkiff,”Denial-of-service in wireless sensor networks: Attacks and defenses,” (2008).

[4] Yangcheng Huang and Saleem Bhatti,“Fast converging distance vector routing for wireless mesh networks” ICDCS, (2008)

[5] Jing Deng, Richard Han, Shivakant Mishra,“INSENS: Intrusion-tolerant routing for wireless sensor networks” (2006).

[6] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig,”Secure sensor network routing: A clean-slate approach” (2006).

[7] Jing Deng, Richard Han, and Shivakant Mishra, “Defending against path based DoS attacks in wireless sensor networks” ACM workshop on security of ad hoc and sensor networks, (2005).

[8] Rahul C. Shah and Jan M.Rabaey,”Energy aware routing for low energy ad hoc sensor networks”(2002).