Efficient Prevention of Vampire Attack in Ad-hoc Wireless Sensor Network

Ms. Raisa I. Mulla[1], Prof. Rahul N. Patil[2]

[1]PG Scholar, Computer Engineering Department, Bharati Vidyapeeth College Of Engineering, Navi-Mumbai, India
[2]Assistant Professor, Computer Engineering Department, Bharati Vidyapeeth College Of Engineering, Navi-Mumbai, India

Email: raisamulla38@gmail.com

Abstract— Ad-hoc low-power wireless networks are the challenging analysis direction in sensing and pervasive computing. Wireless Senor Network (WSN) basically use for security and energy efficiency. Early work on security in this area has been focused on denial of service (DOS) at the routing or medium access control (MAC) levels. Previously, the resource depletion attacks are considered as a routing problem, under this model are classified in to a new group called "Vampire attacks". This difficult work examine thoroughly the identification of resource depletion attacks at the routing protocol layer and in the application layer, which completely disable networks by quickly exhausting nodes' battery power. Vampire attacks are not a protocol specific and they do not rely on design properties but rather exploits properties of protocol classes of routing protocols. Vampire attacks are liable to be influenced or harmed by a particular thing, which are disastrous, hard to find, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. A single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes, happens in worst case. In this work a detection and control strategy is proposed for these vampire attacks, along with a secure packet forwarding mechanism, which will keep safe from harm and danger Ad-hoc wireless nodes from power exhaust due to Vampires at packets forwarding level.

Keywords— Medium Access Control(MAC), Denial of Service(DOS), Routing Protocol, Ad-hoc Wireless Network, Wireless Sensor Network(WNS), Wireless Network Security.

INTRODUCTION

A group of two or more computers are communicate together are known as a network. Basically networks are classified into three different networks Local Area Network (LAN), Wide Area Network (WAN), and Metropolitan Area Network (MAN). Large number of sensor nodes that are deployed in a particular region known as sensor network. To monitor physical and environmental condition such as Temperature, Sound, Pressure, etc and to cooperatively pass their data through the network to a main location is called a Wireless Sensor Network (WSN). Wireless Sensor Network is a distributed network. Basic characteristic of wireless sensor network is a resource constrains.

A wireless ad hoc sensors network spreads a number of sensor nodes across a geographical area. Ad-hoc wireless sensor networks (WSNs) gives honor to be introduce new applications, such as on demand computing power, continuous connectivity, and quickly spread communication for military and responders. Communication among nodes of network without any pre-existing infrastructure is a characteristic of an ad hoc sensor network. WSNs become more excellent to the day to day functioning of people and organizations, availability faults become moderately good, lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a decisive property, and should hold even under malicious conditions. Due to their ad-hoc organization, wireless ad-hoc networks are exposed to denial of service (DOS) attacks, and a research has been done to enhance survivability. These are secure to attacks on the short-term availability of 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. In this consider how routing protocols, even those designed to be secure, lack protection from these attacks, since they exhaust the life from networks nodes. These attacks are distinct from denial of services (DOS) , reduction of quality(ROQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network.

Vampire attacks are exploits general properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Vampires use protocol-compliant messages, these attacks are much hard to detect and prevent. Each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Ad-hoc networks not provide support to wired gateway. Flooding for forwarding data use in Ad-hoc network. An Ad-hoc network provide support to any set of networks where all devices have equal status on a network and are free to associate with any other Ad-hoc network device in link range. Ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks and network device's ability to maintain link status information for any number of devices in a hop range. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly.

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The basic challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Contributions—

The basic three primary contributions make this paper.

a. To evaluate the vulnerabilities of existing routing protocol when done battery depletion attack on routing layer. An existing secure routing protocol such as Ariadne, SAODV, and SEAD are vulnerable to Vampire attack. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return invalid network path, but vampire do not disrupts or alter discovered paths instead using existing valid network paths and protocol compliant messages. Protocols that maximize power efficiency are also inappropriate and cannot optimize battery power usage.
b. Simulation Results of quantifying performance of several representative protocols in the presence of Vampire (Single insider adversaries).
c. Modification of an existing sensor network routing protocol is made to prevent the damage caused by vampire attack during packet forwarding phase.

A. Classification

Denial of service (DOS) Attack is malicious attempt by a single person to cause a victim, site or node to deny service to its' customer. Denial of service is an attack, where a victim can cause multiple of 10 times of the CPU time to transmit a data packet, but whereas honest node uses multiple of 1 time of CPU time to transmit the same data packet. A composing a shortest path from source to destination and transmit data packet to next hop in multi hop routing protocol. Composing and transmitting a malicious message that select the longest path which consumes more energy of the network than if an honest node transmit a message that select the shortest path which consumes less energy of the network is defined as vampire attack. The ratio of network energy used in honest case as well as malicious case can measure strength of attack.

B. Protocols and Assumptions

Effects of vampire attacks on link-state, distance vector, source routing, geographic, beacon routing protocols and logical ID-based sensor network routing protocol proposed by Parno et al. These all protocols are subset of routing solution and also prevent from vampire attack. There are two different routing protocols such as on –demand routing protocol in which topology is discovered during transmission time and static protocol in which topology is discovered during an initial phase. To attack on many honest nodes few vampires are allow sending packet automatically. Adversaries are nothing but a malicious insider and have same resources and level of network access as honest nodes. Adversary corrupts a number of honest nodes after network developed. Honest nodes are safe when vampire sleeps and vulnerable while active.

C. Overview

In this paper, defines a series of increasingly damaging vampire attacks, evaluate vulnerability of several protocols, and suggest how to improve flexibility. In source routing protocol, source suggested path for forwarding packets and show how malicious packet source can specify paths through the network, which are far longer than optimal thus wasting energy at intermediate nodes that forward the packet from source. In routing schemes, each node independently made forwarding decision. In this paper suggest, how directional antenna and wormhole attack can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all and increasing network wide energy expenditure. End of this paper, route and topology discovery phases can target by an adversary at packet forwarding phase.

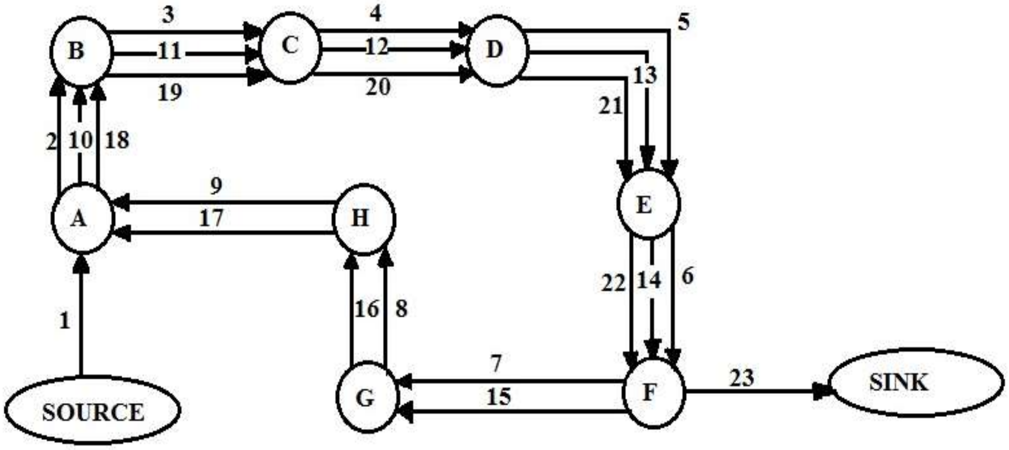

Fig.1. Carousal Attack

CAROUSAL ATTACK:

In this type of attack, adversary constructs routing loops. A malicious node sends a packet with a route composed as a series of loop with the same node appears in the route many times this attack called Carousal attack. It sends packets in circles. In carousal attack, targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

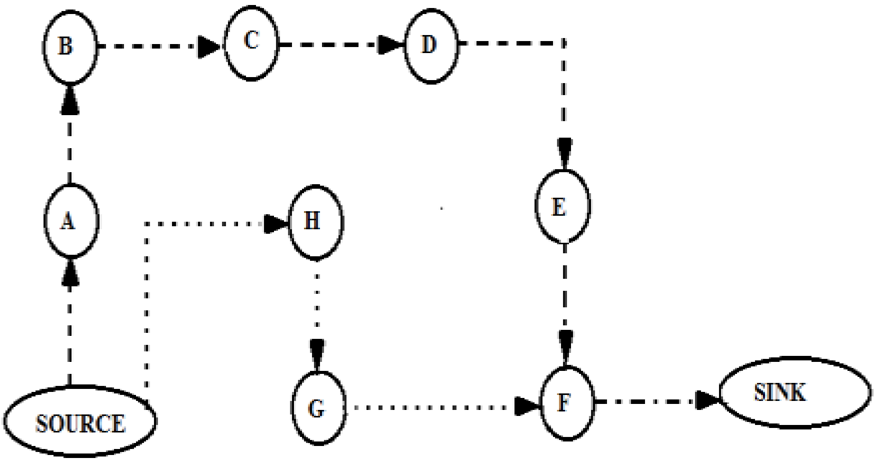

Fig.2. Stretch Attack

STRETCH ATTACK:

In this type of attack, adversary construct artificially long route. If shorter route being available then also a malicious node constructs artificially long routes from the source to destination. A number of nodes that is independent of hop count along the shortest path between the adversary and packet destination which causing packets to be processed and it increases packet path lengths.

SYSTEM METHODOLOGY

The network is collection of many nodes. To detect vampire attack energy based mechanism is implemented. After constructing a network, a malicious message will be send from attacker node to normal node. Normal node consumes more energy than the normal message level so it assumes that node is affected by an attack. If affected node is identified in the network that node eliminated from network. Hence attack node unable to communicate with normal node in the network. Present system uses one way hash chain, which limits packet transmission rate. Malicious nodes are drains their own batteries and reduce energy usage. Present System & All leaf nodes are physical nodes in network and virtual addresses corresponds to their position in the network. Original version is vulnerable to vampire attacks.

CLEAN-SLATE SENSOR NETWORK ROUTING (PLGP):

Developed By Parno,Luk, Gaustad and Perrig (PLGP). PLGP consist of two phases.

Two phases:

a) Topology discovery Phase

b) Packet forwarding phase

a) Topology Discovery Phase: In this network converges to a single group. Virtual address, public key and certificate are knows by each node. Each node has its own group address of size one, with virtual address zero. Groups merge with smallest neighboring group which may be single node. Example, 1) node 0 and group 0 becomes 0.0, 2) node 0 group 1 becomes 1.0 and so further. Every node broadcast certificate of identity including public key.

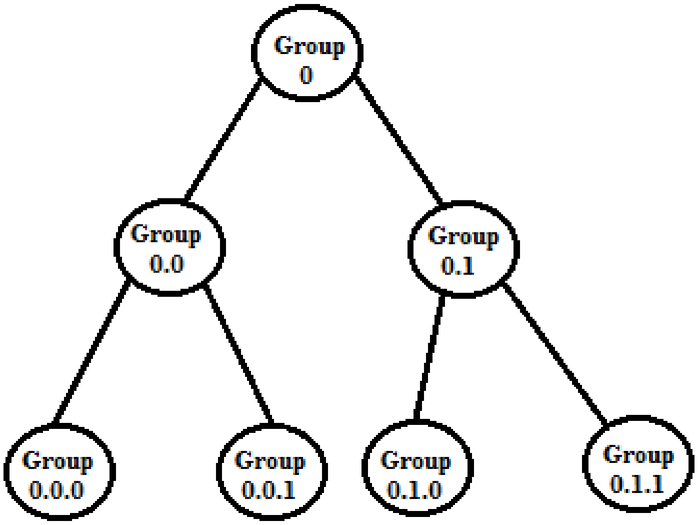

Fig.3. Binary tree of all addresses in the network

b) Packet forwarding phase: In packet forwarding phase, each node independently made all decision. A node when receives a packet determines next hop by finding the most significant bit of its address that differs from the message originators address. Every forwarding event minimize the logical distance to destination.

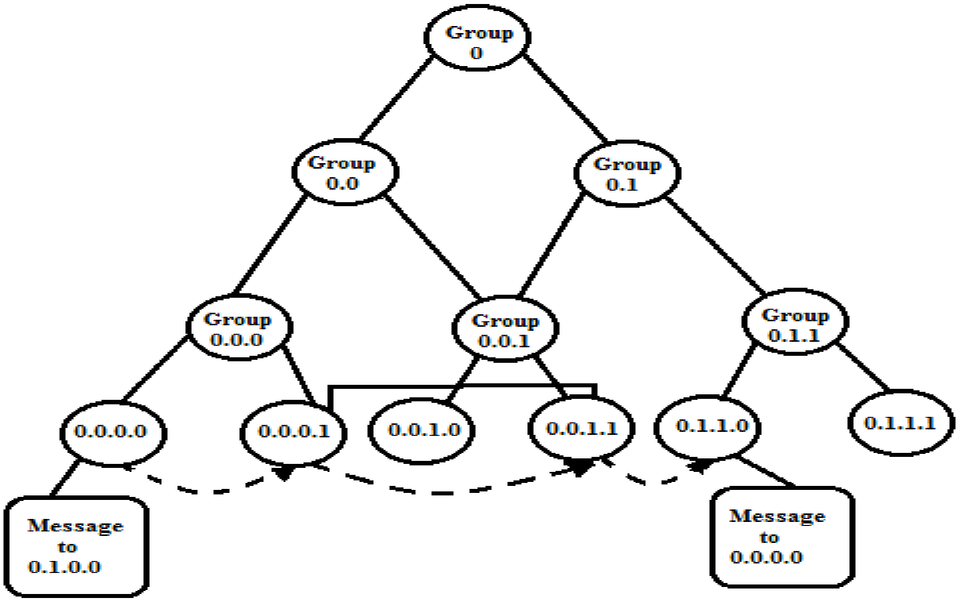

Fig.4. Final address tree for fully-converged 6-node network

PLGP in presence of vampires:

In the worse case, if packet returns to vampire as it can reroute. Theoretical energy increase of O(d) where d is the network diameter and N the number of network nodes. Vampire moves packet away from the destination. But honest node knows only its address and destination address. Honest node may be farther away from the destination than malicious nodes. Forwarding nodes don't know the path of a packet and allowing adversaries to divert packet to any part of the network.

Provable Security against vampire attacks (**No-backtracking property**):

No-backtracking implies vampire resistance. Nodes keep track of route cost. More formally: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network.

PLGP WITH ATTESTATION (PLGP-a) PHASE:

Every PLGP packet has verifiable path history. 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. PLGP with attestations (PLGP-a) 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. Add a verifiable path history to every PLGP packet.

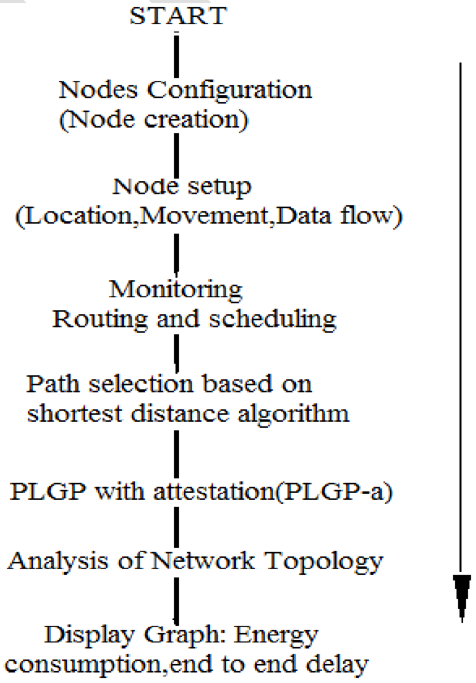
START
Nodes Configuration
(Node creation)
Node setup
(Location,Movement,Data flow)
Monitoring
Routing and scheduling
Path selection based on
shortest distance algorithm
PLGP with attestation(PLGP-a)
Analysis of Network Topology
Display Graph: Energy
consumption,end to end delay

Fig.5. Proposed flow

M-DSDV NETWORK ROUTING

M-DSDV is a modified destination sequence distance vector. It is proactive network routing protocol. Proactive means utilizes more battery power and bandwidth. It helps to protect from Vampire attack during packet forwarding phase. Existing DSDV is designed basically to resolve routing loop problem. M-DSDV consist of both packet forwarding phase as well as topology discovery phase. A proper or legal network node has a unique certificate of membership. A unique certificate of membership includes it's public key and code word. Code word assigned by a trusted offline authority before spread. For transmitting data packets, topology discovery of the neighboring nodes begins.

Each node knows itself only very well. To discover their neighbors, nodes use local broadcasting scheme. In local broadcasting scheme certificate identity verification is done to isolate external unauthorized nodes from the network. If node is honest node, they know it's neighbor node's address and public key.

For example source node S, want to send a data packet to destination D, initially construct and broadcast a route request (RReq) packet consisting of (source address, destination address, sequence number, next hop, metric, index number and time to live) fields. Source address and destination address are internet protocol address, sequence number is used to differentiate new route from stale route, each node maintained next hop and metric are a local counter and each time RReq is broadcasted, index number is initialize to zero is basically used to keep track of the loops the packet has made, and lastly time to live field is used as a clock which increments whenever a RReq packet is sent.

On receipt of RReq, intermediate nodes inspect it to see if it is a duplicate, in which case it is rejected. If not pair is entered into the local history table. The destination address looked up in the routing table, if a fresh route to it is known an RRep a route reply packet is sent back to S. This also creates a backward route towards S. When destination receives RReq, it sends back an RRep packet to the node from which it got the first RReq packet.

The format of the route reply packet includes (Source address, Destination address, Destination sequence, index number, life time). In this source address, destination address and index number are copied from the incoming RReq packet, but the destination sequence number is taken from its counter in memory. The life time field indicates how long the route is valid.

On receipt of RRep, intermediates nodes on the way back, inspect the packet and create a backward route towards destination. Intermediate nodes that got the original RReq packet but were not on the reverse path discard the reverse route table entry when associated timer expires. When the next hop link in the routing table entry breaks, all active neighbors are informed by means of RERR packets which updates the sequence number. RERR packets are also generated when a node X is unable to forward packet P from node S to node D on link (X, Y). Incremented sequence number N is include in RERR. When node S receives the RERR ,it initiates a new route discovery for D using the sequence number that is at least as large as N

In the presence of vampires carousal attack and stretch attack can be prevented by using index number. In carousal attack packet traversed through the shortest path of network. Index number stored on the packet header and index number stored on local routing table of the node. In stretch attack the nodes keep track of route "Metric" and when acknowledgement return back , the route metric value and index number which indicates hop count, can be verified. If the index value > the metric value it concludes stretch attack as occurred. Clean slate sensor routing or PLGP and proposed PLGP-a help to prevent from attack on wireless ad hoc sensor network.

CONCLUSION

Vampire attack has been defined as a class of resource consumption attacks that use routing protocol to completely disable ad hoc wireless sensor networks by exhaust nodes' battery life. Resource consumption attacks are not protocols specific. Network energy expenditure increased when forwarding phase attack has been proposed. Clean Slate Sensor Network Routing (PLGP) is first routing protocol that reduces damage from Vampire attack by verifying packets consistently make progress towards their destination. M-DSDV routing protocol used in packet forwarding phase, bounds damage from Vampire attacks.

REFERENCES:

[1] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[2] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, andScott F. Midkiff, Effects of denial-of-service attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.

[3] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 7 (2008), no. 1.

[4]] 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.

[5] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang, Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM, 2005.

[6] David B. Johnson, David A. Maltz, and Josh Broch, DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, Ad hoc networking, 2001.] Volkan Rodoplu and Teresa H. Meng, Minimum energy mobile wireless networks, IEEE Journal on Selected Areas in Communications 17 (1999), no. 8.

[7] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on demand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002), no. 3.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.

[9] Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.

[10] Rushing attacks and defense in wireless ad hoc network routing protocols, WiSE, 2003.

[11] Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003