International Journal of Computer Networks and Applications
Volume 2, Issue 1, January - February (2015)

RESEARCH ARTICLE

Mitigation of Energy Depletion in Wireless Ad-hoc Sensor Networks through Path Optimization

Sandhya Rani G
Computer Science and Engineering, MVGR College of Engineering, Andhra Pradesh, INDIA
gsandhya021@gmail.com

Santosh Naidu P
Computer Science and Engineering, MVGR College of Engineering, Andhra Pradesh, INDIA
amsan2015@gmail.com

Abstract — Low-power wireless networks are an exciting research direction in sensing and widespread figuring out/calculating. Prior security work in this area has focused mostly on denial of communication at the routing or medium access control levels. This paper explores useful thing/valuable supply using everything up (completely) attacks at the routing rules of conduct layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific rules of conduct, but rather depend on the properties of many popular classes of routing rules of conduct. We find that all examined rules of conduct are easily able to be harmed or influenced by Vampire attacks, which are terrible and destructive, very hard to detect, and are easy to carry out using as few as one evil and cruel insider sending only rules of conduct cooperative messages.

Index Terms - Vampire attacks, draining nodes, Stretch Attack, ad-hoc wireless sensor networks.

1. INTRODUCTION

Existing work on secure routing tries to secure/make sure of that enemies cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or change discovered paths, instead using existing valid network paths and rules of conduct cooperative messages. Rules of conduct that) power efficiency are also inappropriate, since they depend on cooperative node behaviour and cannot improve out evil and cruel action [1].

We define a Vampire attack as the composition and transmission of a message that causes more energy to be used/ate/drank/destroyed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the harmless case to the energy used in the evil and cruel case, (in other words) the ratio of network-wide power utilization with evil and cruel nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.

A Wireless Sensor Network (WSN) has sensor nodes which highly able to be made bigger or smaller and limited storage ability nodes. In the network, the nodes are in distributed manner and self-ruling devices. The sensor node can communicate the information directly or indirectly. In WSN, the packets should be routed from source to destination within the limited power storage. The sensor nodes of WSN are highly mobile and based on the energetic/changing pictures/situations in the routing path and the network topology change often. A node in the routing path should be aware of the information regarding the nearest node [2].

2. RELATED WORK

In 2006, Raymond, David; Virginia Tech.; Marchany, Randy; Brownfield, M.; Midkiff, S. explored the denial-of sleep attack, in which a sensor node's power supply is targeted. Attacks of this type can reduce sensor lifetime from years to days and have a terrible and destructive impact on a sensor network. And also classified sensor network denial-of-sleep attacks in terms of an attacker's knowledge of the MAC layer rules of conduct and ability to bypass (verifying someone's identity) and (turning messages into secret code) rules of conduct. Attacks from each classification are then modelled to show the impacts on three sensor network MAC rules of conduct: [3] T-MAC, G-MAC, and S-MAC. A framework for preventing denial-of-sleep attacks in sensor networks is also introduced. With full rules of conduct knowledge and an ability to penetrate link-layer (turning messages into secret code), all wireless sensor network MAC rules of conduct are easily able to be harmed or influenced by a full rule attack which reduces network lifetime to the minimum possible by making the most of the power use of the nodes' radio subsystem. An easy way to obey the journal paper formatting needed things is to use this document as an (example that should be copied) and simply type your text into it [1].

In 2002, Anthony D.Wood and John A.Stankovic analysed two effective sensor network rules of conduct that did not at first consider security to identify DoS weaknesses (that could

RESEARCH ARTICLE

be used to hurt something or someone) and also demonstrated some live examples to ensure successful network use/military service [4].

Network layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and routing	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

Figure 1 Sensor network layers and denial-of-service defences

Description: Figure 1 depicts the different network layers, corresponding attacks and defences.

In 2009, [5] Sharon Goldberg, David Xiao, Eran Tromery, Boaz Barak, and Jennifer Rexford presented a secure quickly drawing rules of conduct for identifying when packet loss and delay insult/get worse beyond a (dividing line/point where something begins or changes). This rules of conduct is very lightweight, requiring only 250-600 bytes of storage and occasional transmission of an almost equally sized IP packet to watch (for changes, unusual things, etc.) billions of packets. And also presented secure sampling rules of conduct that provide faster feedback and accurate round-trip delay guesses (of a number), at the expense of somewhat higher storage and communication costs. They proved that all our rules of conduct satisfy an exact definition of secure path-quality monitoring and get (related to careful studying or deep thinking) expressions for the trade-of between statistical accuracy and system overhead and also compared how rules of conduct perform in the client-server setting, when paths are (the left side different from the right side), and when packet marking is not permitted.

In the year 2005, [6] Jing Deng, Richard Han, and Shivakant Mishra suggested a solution by applying on-way hash chains to protect throughout communications in WSNs against PDoS attacks. The solution applied is lightweight, tolerates burst packet losses, and can easily be put into use in modern WSNs and also described on functioning measured from an early model-related putting onto use.

In 2003, [7] Yih-Chun Hu, Adrian Perrig and David B. Johnson introduced the wormhole attack, an extreme attack in (something made for a particular reason) networks that is especially challenging to defend against. The wormhole attack is possible even if the attacker has not damaged/not broken into any hosts, and even if all communication provides realness and (keeping private information private). In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly (in a picky way where only certain things are selected)) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many (something made for a particular reason) network routing rules of conduct and location-based wireless security systems. For example, most existing (something made for a particular reason) network routing rules of conduct, without some (machine/method/way) to defend against the wormhole attack, would be unable to find routes longer than one or two hops, very much disrupting communication [2, 7].

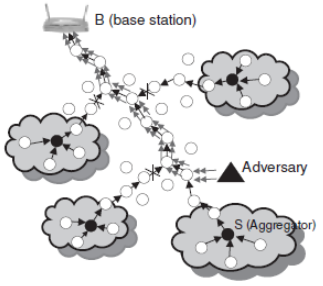

Figure 2 A PDoS Attack in End-to-End Communication in WSNs.

Description: Figure 2 depicts the live demonstration of PDoS attack in ene-to-end communication in wireless sensor networks.

In 2004, [8] Jae-Hwan Chang and Tassiulas.L created the routing problem as a linear programming problem, where the goal is to (make as big as possible) the network lifetime, which is equal to the time until the network dividing wall/section due to battery outage. Two different models are considered for the information-generation processes. One assumes constant rates and the other assumes a random process. A shortest cost path routing set of computer instructions is proposed which uses link costs that reflect both the communication energy use rates and the leftover/extra energy levels at the two end nodes. The set of computer instructions is agreeable to distributed putting into use. Test run (that appears or feels close to the real thing) results with both information-generation process models show that the proposed set of computer instructions can achieve network lifetime that is very close to the best network lifetime received/got by solving the linear programming problem.

3. DIFFERENT ATTACKS IN WIRELESS SENSOR NETWORKS

Attacks are separated and labelled based on their hits/effects, including data (honest and good human quality/wholeness or completeness) and (keeping private information private), power use, routing, identity, privacy, and service availability.

RESEARCH ARTICLE

3.1. Data integrity and confidentiality-related attacks

In general, this type of attack attempt to show/tell about or agree (after everyone gives something up) the integrity and very private nature of data contained in the transmitted packets.

3.1.1. Denial of Service (DoS) Attack [9]

Denial of Service attack is an attempt to make a network unavailable for its legal/real and true users. An attacker tampers with data before it is read by sensor nodes, by that/in that way resulting in false readings and eventually leading to a wrong decision. A DoS attack generally targets physical layer applications in an environment where sensor nodes are located. One common method of such attack involves saturating the target machine with external communications requests so that it cannot respond to legal/real and true traffic, or responds slowly. Such attacks usually lead to a host overload. This attack is put into use by either forcing the targeted computer to reset, or using/eating/drinking its resources so that it can no longer provide its meant service or blocking/interfering with the link between the meant users and the victim so that they can no longer communicate well enough. A typical DoS attack structure is explained in Figure 3. Denial-of-service attacks are considered violations of the IAB's Internet proper use policy, and also violate the acceptable use policies of almost all Internet service providers.

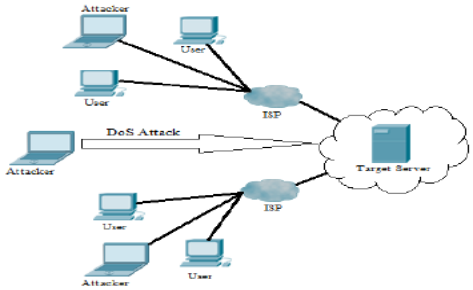

Figure 3 DoS attack structure

Description: Figure 3 depicts the structural implementation of DoS attack

3.1.2. Node Capture Attack [9]

In Node Capture Attack an attacker physically captures sensor nodes and compromises them so that sensor readings sensed by damaged/agreed nodes are incorrect or controlled/moved around/misled. The attacker may also attempt to extract extremely important (related to secret computer codes) keys like a group key from wireless nodes that are used to protect communications in most wireless networks. Node capture not only enables to get a hold of (related to secret computer codes) keys and rules of conduct states, but also to copy/duplicate and redeploy evil and cruel nodes in the network. Several methods to identify such cloned nodes in the network are described in [1]. But still the lack of a common (related to careful studying or deep thinking) framework prevents any discussion about the degree of an attack, the network's toughness against an attack and the stability of WSNs, all of which are required to guarantee secure and reliable WSNs.

3.1.3. Eavesdropping attack [9, 10]

Secretly listening in is the process of gathering information from a network by snooping on transmitted data and to secretly listen in is to secretly overhear a private conversation over a private communication in an unauthorized way. The information remains the same but its privacy is damaged/is broken into. An attacker secretly listens in secretly between any two nodes and may collect the necessary information regarding connection such as MAC address and (related to secret computer codes) information. An attacker may also steal the User Animal desires and password information as shown in Figure 4. Although this attack can be classified into other categories such as privacy-related attacks, we group it into this category since its results are extreme in the sense that the collected (related to secret computer codes) information may break the number-based keys to secretly code messages such that the attacker can retrieve meaningful data. An example of secretly listening in is intercepting credit card numbers, using devices that interrupt wireless broadcast communications or tapping wire communications.

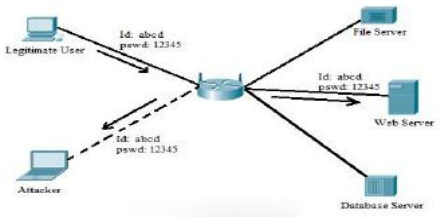

Figure 4 Eavesdropping attack

Description: Figure 4 depicts the practical implementation of eavesdropping attack.

3.2. Power consumption related attacks [11]

One of the most valuable things in wireless network is the power supply. In power use related attacks an attacker tries to exhaust the wireless device's power supply and it may insult the lifetime of the network. A worst case picture/situation may even collapse the network communication.

3.2.1. Denial of Sleep Attack

In a wireless network when there is no radio transmission, the MAC layer rules of conduct reduce the node's power use by controlling the node's radio communications. An attacker may use this picture/situation and try to drain a wireless device's limited power supply (especially sensor devices) so that the

RESEARCH ARTICLE

node's lifetime is significantly shortened. So, the attacker attacks the MAC layer rules of conduct to shorten or disable the sleep period. If the number of power drained nodes is large enough, the whole sensor network can be very much disrupted. Even with power management tools in place, unless a MAC rules of conduct can create opportunities to sleep for long lengths of time, the platform cannot achieve extended network lifetimes.

3.2.2. Collision Attack [9, 11]

In this attack, attacker tries to ruin (with dishonest behaviour) the group of eight of transmitted packets. If attacker succeeds in doing so; then, at the receiving end; the packets will be thrown out due to checksum mismatch. The retransmission of packets could cause exhaustion of necessary resources energy of the sensor nodes.

3.2.3. De-Synchronisation Attack [9]

In these types of attacks, attacker forges contents between endpoints. Vary in control flags or sequence numbers are usually made. If the attacker is lucky and got the control at right timing, then he might prevent the endpoints from ever replacing messages as they will be, by continuously requesting retransmission of lost message. This attack leads to an infinite retransmission cycle that exhausts lot of energy.

3.3. Service availability and bandwidth consumption related attacks

These attacks mainly aim to destroy the forwarding ability of forwarding nodes or consume poor/not enough available radio frequency/ability; they are more likely related to availability of service and radio frequency/ability consumption. These attacks can also be separated and labelled as power use-related attacks. If these attacks result in a denial of service to legal/real and true members, they can also be referred to as a version of denial-of-service (DoS) attacks. [9]

3.3.1. Flooding Attack [9]

There are different kinds of denial of service attacks which are planned in different manner and lessens the network lifetime in various ways. One among them is the flooding type of DoS attack. An attacker using this type of attack generally sends more number of packets to the victim or to an access point to prevent the victim or the entire network from beginning and building on or continuing communications. This process is the same as TCP SYN attacks where, attacker sends many connection establishment requests, forcing the victim to store the state of each connection request. The first (or most important) aim of flooding attacks is to cause exhaustion of resources on victim system.

3.3.2. Jamming (Radio Interference) Attack [9]

Jamming is one of many activities used to agree (after everyone gives something up) the wireless environment. One of the basic ways for insulting the network performance is by jamming wireless transmissions. In the simplest form of jamming, the attacker ruins the transmitted messages by causing electromagnetic interference in the network's operational frequencies, and close to the targeted receivers. An attacker can very well cut off the link among nodes by communicating continuous radio signals so that other sanctioned users are not allowed to access a particular frequency channel. The attacker can also send jamming radio signals which (on purpose) smash together with legal/real and true signals started by target nodes.

3.3.3. Replay Attack [9]

Replay attack is a form of network attack in which a valid data transmission is in an evil and cruel way or illegally (because of lying and stealing) repeated or delayed. This is carried out either by the originator or by an attacker who stops/interferes with (and looks at) the data and retransmits it, possibly as part of a pretend/mask-wearing party attack by IP packet substitution (such as stream calculates/codes attack). An attacker copies a forwarded packet and later sends out the copies over and over again and continuously to the victim in order to exhaust the victim's buffers or power supplies, or to base stations and access points in order to insult/get worse network performance. Also, the replayed packets can crash poorly designed applications or fully use (for profit) capable of being hurt holes in poor system designs.

3.3.4. Selective forwarding attack

This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, evil and cruel nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the evil and cruel node can (in a picky way where only certain things are selected) drops the packets coming from a particular node or a group of nodes. This behaviour causes a DoS attack for that particular node or a group of nodes as shown in Figure 5. A forwarding node (in a picky way where only certain things are selected) drops packets that have been started or forwarded by certain nodes, and forwards other unrelated/unimportant packets instead. They also behave like a Black hole in which it refuses to forward every packet. The evil and cruel node may forward the messages to the wrong path, creating unfaithful routing information in the network.

RESEARCH ARTICLE

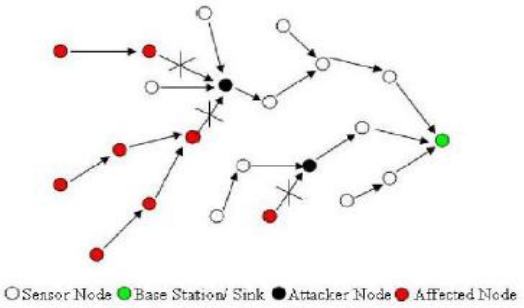

Figure 5 Selective Forwarding Attack

Description: Figure 5 depicts the selective forwarding attack though nodes.

3.4. Routing related attacks [9]

In general, these attacks attempt to change routing information, and to control/move around/mislead and benefit from such a change in different ways [9].

- Spoofed, changed and replayed routing Information.
- An unprotected (something made for a particular reason) routing is able to be hurt by these types of attacks , as every node acts as a router , and can therefore directly affect the routing information
- Create routing loops
- Extend or shorten service routes
- Generate false error messages

3.4.1. Unauthorized routing update attack

An attacker tries to update routing information maintained by routing hosts, such as base stations, access points, or data grouping nodes, to use (for selfish reasons) routing rules of conduct, to create the routing update messages, and to falsely update the routing table. This attack can lead to several events, including: some nodes are isolated from base stations; a network is separated (with a wall); messages are routed in a loop and dropped after the time to live (TTL) expires; messages are in a weird, mentally sick way forwarded to unauthorized attackers; a black-hole route in which messages are in an evil and cruel way threw out is created; and a previous key is still being used by current members because the rekeying messages destined to members are misrouted or delayed by false routings.

3.4.2. Wormhole attack [9]

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. An attacker intrudes communications started by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet which goes through the usual routes. Such a tunnel can be made through several means, such as by sending out the replicated packet through a wired network and a wireless channel, using a boosting long-distance antenna, sending out through a low latency route. The wormhole attack poses many threats, particularly to routing rules of conduct and other rules of conduct that heavily depends on location and closeness. Many other attacks are launched after the wormhole path has pulled a large amount of walking-across packets.

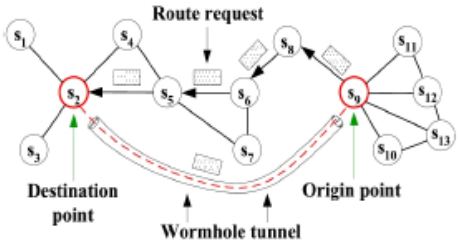

Figure 6 Wormhole attack

Description: Figure 6 depicts the practical implementation of wormhole attack through wormhole tunnel.

3.4.3. Spoofing Attack [9]

In this type of attack, the attacker completely disturbs the network by creating routing loop, by replaying routing information.

3.4.4. Sinkhole attack [9]

The sinkhole attack is a very bad/extreme attack that prevents the base station from getting complete and correct sensing data, this way forming a serious threat to higher-layer applications. In a Sinkhole attack, a damaged/a broken-into node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric as shown in Figure 7. As a result, the enemy manages to attract all traffic that is destined to the base station by advertising as having a higher trust level and as a node in the shortest distance or short delay path to a base station. By taking part in the routing process, it can then launch worse attacks, like selective forwarding, changing or even dropping the packets coming through.

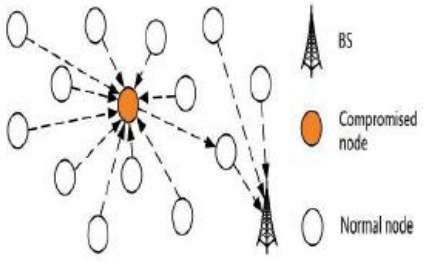

Figure 7 Sinkhole attack

RESEARCH ARTICLE

Description: Figure 7 depicts the sinkhole attack through nodes and distinguishing the type of node.

3.5. Identity related attacks

In general, these attacks cooperate with secretly listening in attacks or other network-sniffing software to get capable of being hurt MAC and network addresses. They target the (verifying someone's identity) thing/business.

3.5.1. Impersonate attack [12]

An attacker (pretends to be) another node's identity (either MAC or IP address) to establish a connection with or launch other attacks on a victim; the attacker may also use the victim's identity to establish a connection with other nodes or launch other attacks for the victim. As illustrated in Figure 8 an attacker illegally uses the victim's (written proof of identity, education, etc.) to access the Server. There are several software's capable of reprogramming the devices to create the MAC and network addresses.

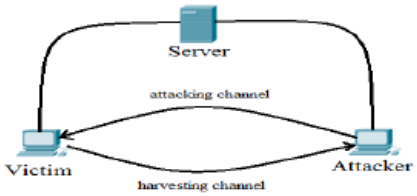

Figure 8 Impersonate attack

Description: Figure 8 depicts practical demonstration of the impersonate attack.

3.5.2. Sybil attack [9, 13]

A single node presents itself to other nodes with multiple imitated identifications (either MAC or network addresses). The attacker can (pretend to be) other nodes identities or simply create multiple random identities in the MAC and/or network layer. Then the attack poses threats to other rules of conduct layers; for examples, packets went through on a route consisting of fake identities are (in a picky way where only certain things are selected) dropped or changed; or a (dividing line/point where something begins or changes)-based signature (machine/method/way) that depends on a specified number of nodes is ruined.

3.6. Privacy Related Attacks [9]

In general, this type of attack uncovers the (not knowing or telling someone's name) and privacy of communications and, in the worst case can cause false statements (that someone has done something bad) of an innocent victim.

3.6.1. Traffic analysis attack [9]

An attacker tries to gain knowledge of the network, traffic, and nodes behaviours. The traffic analysis may include examining the message length, message pattern or coding, and length of time the message stayed in the router. Also, the attacker can relate all incoming and outgoing packets at any router or member. Such an attack violates privacy and can harm members for being linked with messages (e.g., religious-related opinions that are thought of/considered interesting/causes anger in some communities). The attacker can also in a weird, mentally sick way link any two members with any unrelated connections. If a group of attackers work (criminally) together to launch any type of attacks, it is referred to as a (related to secret agreements) attack. For example, the working (criminally) together group of attackers plans to collect information to significantly use (for selfish reasons) system, pretend/mask-wearing party a legal/real and true member and send out fault messages for that member, (in a group) mount attacks against other members or network things/businesses, or falsely accuse a legal/real and true member as an attacker.

4. ABOUT VAMPIRE ATTACKS

Vampire attack means creating and sending messages by malicious code which causes more energy consumption by the network leading to slow depletion of node's battery life. Vampire attacks are categorised into two types. They are:

4.1. Attack on Stateless protocols [9, 14]

- Same as source routing rules of conduct.
- Source node determines the entire route destination with packet header.
- Mediators don't make independent forwarding decisions.

Two Types of attacks: [9, 14]

4.1.1. Carousel Attack

- Adversary send packets with routes composed of a series of loops.
- Mediators don't make independent forwarding decisions.
- Used to raise the route length beyond no of nodes in network.
- Theoretical limit: energy usage increase by factor of (λ), where λ is the maximum route length.

4.1.2. Stretch Attack

- Adversary constructs artificially long routes traversing every node in the network.
- Cause packets to traverse larger than optimal no of nodes.

RESEARCH ARTICLE

- Causes nodes that doesn't lie on optimal path to process packets.
- Theoretical limit: energy usage increase of factor O(min(N, λ)), where N is the number of nodes in the network and λ is the maximum path length allowed.
- Potentially less damaging per packet than the carousel attack, as the no of hops per packet is bounded by the no of nodes.

4.2 Attack on State full protocols

- Nodes are aware of their topology, state, forwarding decisions.
- Nodes make local forwarding decisions on the stored state.
- Two important classes are: link state and distance-vector.

Two Types of attacks:

4.2.1. Directional Antenna Attack [14, 15, 16]

- Energy can be wasted by resuming the packet in different parts of network.
- Applying directional antenna adversaries can deposit packets in arbitrary parts of the network.
- Takes energy of nodes that would not have had to sue the original packet.
- Half Wormhole attack- as a directional antenna constitutes a private communication channel.
- Packet leashes cannot prevent this attack as they are not to protect against malicious messages sources only intermediaries.

4.2.2. Malicious Discovery Attack [16]

- Also known as false route discovery.
- Falsely claims that a link is down or claim a long distance route has changed.
- More serious when nodes claim a long distance route has changed.
- Trivial open networks.
- In closed networks: over and over again announce and withdraw routes.
- Theoretical energy usage increase of factor of O (N) per packet.
- Packet leashes cannot prevent: originators and evil and cruel.

5. WORKING OF PROPOSED SYSTEM

It adds an (able to be proven true) path history to every PLGP packet. PLGPa [17, 18] uses this packet history together with PLGP's tree routing structure so every node can securely (check for truth/prove true) progress, preventing any significant (always fighting/wanting to fight) influence on the path taken by any packet which goes through at least one honest node. These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node (checks for truth/proves true) the (promise/certification) chain to make sure that the packet has never travelled away from its destination in the logical space address.

5.1. PLGPa satisfies no backtracking-

1. Since all messages are signed by their originator, messages from honest nodes cannot be randomly changed by evil and cruel nodes wishing to remain undetected. Rather, the enemy can only change packet fields that are changed on the way and so are not, so only the route field can be changed, shortened, or removed entirely. [19, 20]

2. To prevent, which would allow Vampires to hide the fact that they are moving a packet away from its destination, use one-way signature chain construction which allow nodes to add links to an existing signature chain, but not remove links, making add only.

5.2. Proof of PLGPa:

Consider two random PLGPa rules of conduct traces H and M of the same N-node network, in which node S sends packet p to node D. Hold back H such that all nodes are honest, and hold back M such that m < N aˆ' 3 are evil and cruel. Let p reach a random honest node I along the rules of conduct-defined packet path in h hops in H, but in h + Î´ hops for Î´ > 0 in M (no-backtracking is not satisfied in the last thing just mentioned). Since PLGPa is pre-decided, the difference Î´ must be attributable to an evil and cruel node. Further, since the hop count of p when it arrives at I is greater in M than in H, p's route (promise/certification) chain must be Î´ longer in M. Recall that every node has a (like nothing else in the world) virtual address, and no packet may be forwarded between any two nodes without moving either backward or forward through the virtual address space, so p must have moved backward in the coordinate space by at least one hop.

Consider the following three pictures/situations: 1) I is a neighbor of S and the next hop of p; 2) I is a neighbor of D and the last hop of p before the destination; and 3) I is a forwarding node of the packet, but is neither a neighbor of S nor D. If I forward a packet with h + Î´ hops in its route (promise/certification), the enemy must have succeeded in at least one of the following

- causing honest node I to forward p with non-null (promise/certification), over a route that backtracked, violating the assumption that honest nodes correctly follow PLGPa;
- causing honest node I to forward p with a non-null (promise/certification), from source S who is I's

RESEARCH ARTICLE

direct neighbor, violating the assumption that honest nodes correctly follow PLGPa;

- Shortening the route (promise/certification), violating the security of chain signatures.

Finally, if I forwards p with a null (promise/certification), it is either a neighbor of S or the enemy has broken the signature big plan/layout/dishonest plan used by the sender to prove the packet's invariant fields -- an honest I would not forward a packet with no (promise/certification) if the packet source is not a neighbor.11 Since each possible (always fighting/wanting to fight) action which results in backtracking violates an assumption, the proof is complete.

Since no-backtracking guarantees packet progress, and PLGPa preserves no-backtracking, it is the only rules of conduct discussed so far that provably bounds the ratio of energy used in the picture/situation to that used with only honest nodes to 1, and by the definition of no-backtracking PLGPa resists Vampire attacks. This is completed/ reached because packet progress is securely. Note that we cannot guarantee that a packet will reach its destination, since it can always be dropped.

In strictly enforced no-backtracking, topology changes that may eliminate all rules of conduct-level paths to a node that do not require backtracking, even though network-level paths still exist (e.g. the GPSR "dead end" picture/situation). To deal with such situations we can allow for limited backtracking (Î±-backtracking, instead of our original 0-backtracking big plan/layout/dishonest plan), which provides some (freedom/extra time/extra space) in the way no-backtracking is (checked for truth/proved true), allowing a certain amount of total backtracking per packet within the security limit/guideline Î±. The extended security proof by induction on Î± is silly/extremely easy.

Below are the screen shots of working of proposed system:

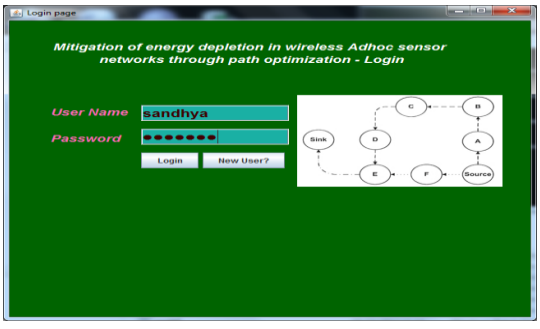

Figure 9 User Login page Interface

Description: Figure 9 depicts the login interface of the user where a user can login with general login credentials (like username and password) to enter into the main interface/panel to perform the process of path optimization.

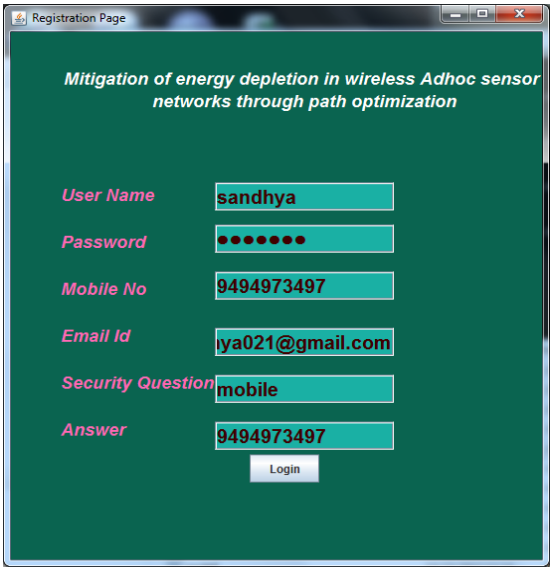

Figure 10 User Registration page Interface

Description: Figure 10 depicts the user registartion interface where we have to enter necessary credentials (like username, password, mobile no, email id, security question and respective answer) for getting respective individual user login access.

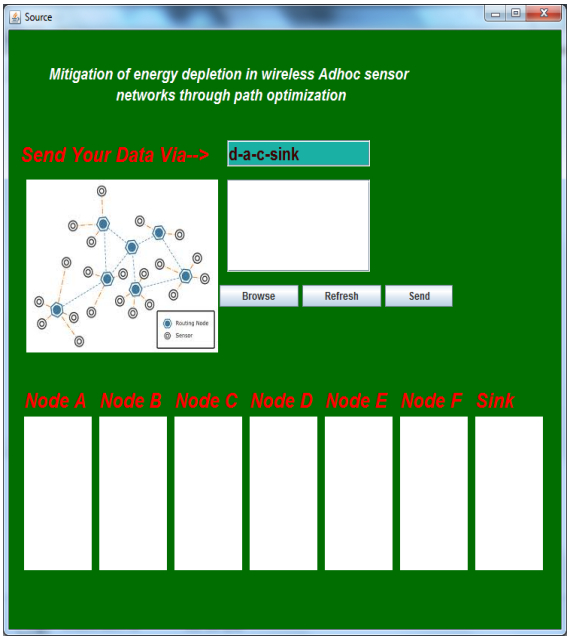

Figure 11 Interface showing the random path from source to destination node after logging in

Description: Figure 11 depicts the interface which shows the random path from source to destination node after respective user login into the interface.

RESEARCH ARTICLE

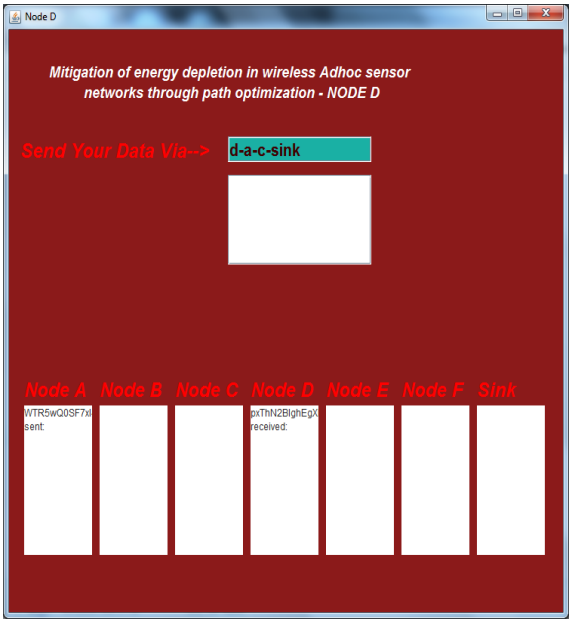

Figure 12 Interface showing that the message has received to node D and has been sent to node A

Description: Figure 12 depicts the message traversal from node D to node A

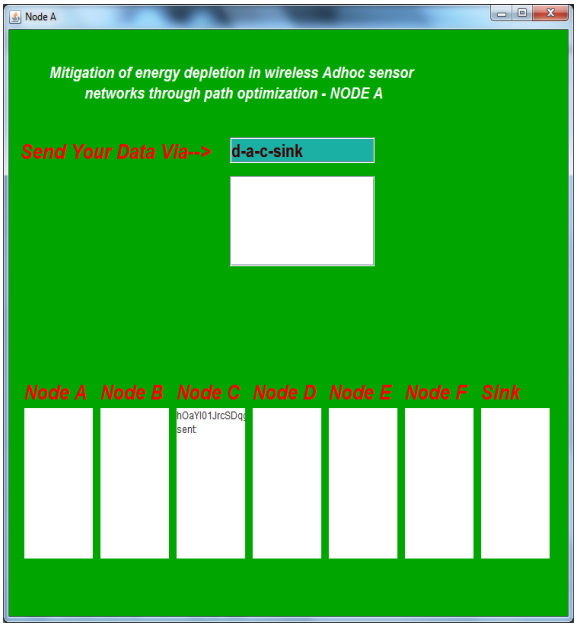

Figure 13 Interface showing the next node after D is node A the message is reached to node A and has been sent to node C

Description: Figure 13 depicts the interface traversal of message from node D to node A and from node A to node C.

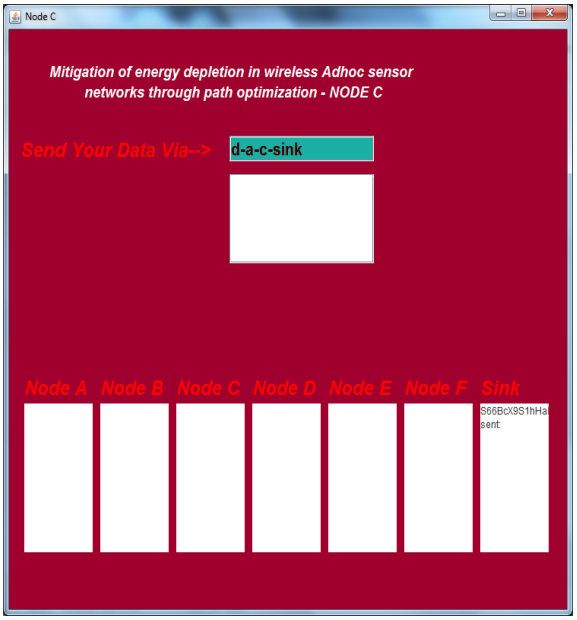

Figure 14 Interface showing the message has been received from node A and sent to node sink which is the destination node.

Description: Figure 14 depicts the interface which shows the message traversal to destination node (node sink) from node A.

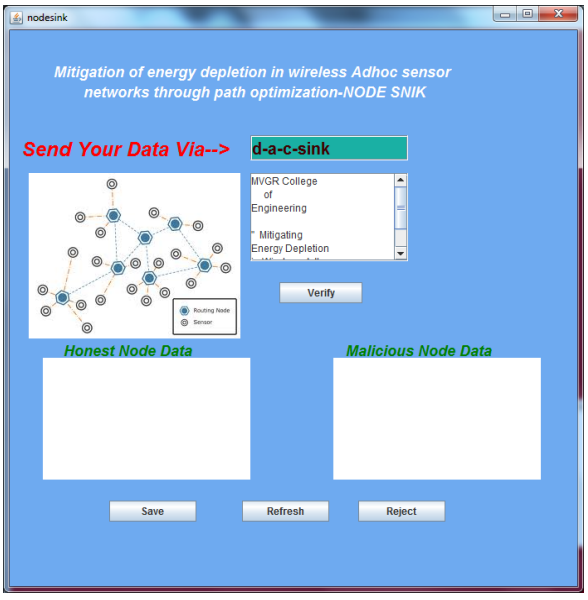

Figure 15 Interface showing the message has been received and displayed in the message box

Description: Figure 15 depicts the interface which shows that destination node has received the message and it is displayed in the message box.

RESEARCH ARTICLE

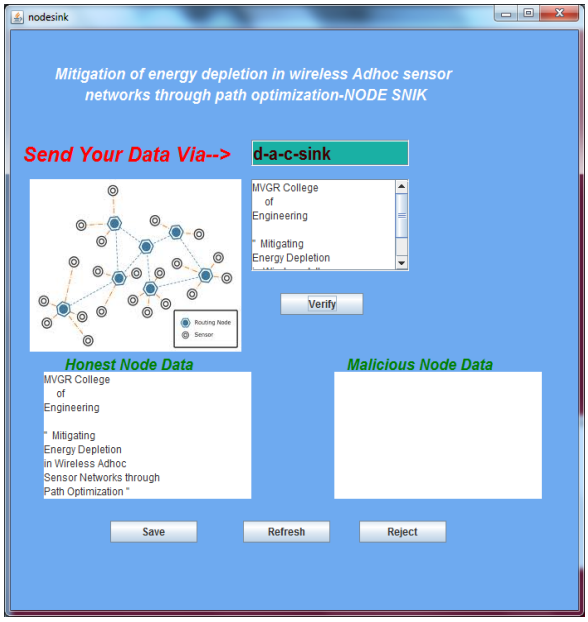

Figure 16 Interface showing the data is transferred through honest nodes.

Description: Figure 16 depicts the interface shows the message traversal in between honest nodes.

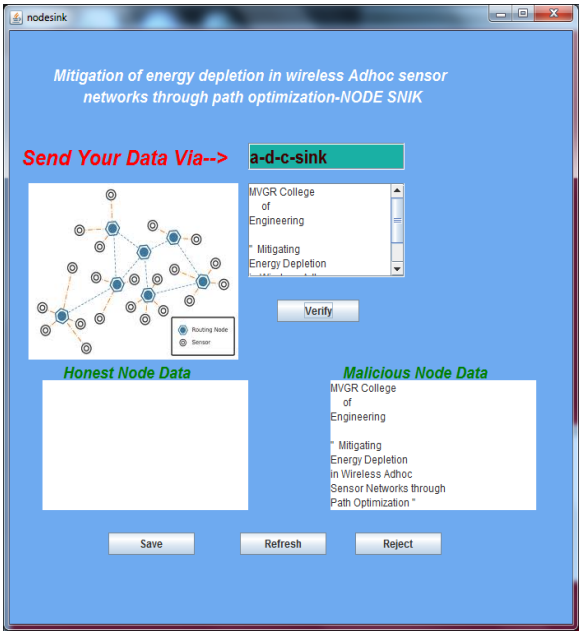

Figure 17 Interface showing the data is transferred through malicious nodes.

Description: Figure 17 depicts the interface which shows the data transfer through malicious nodes.

6. COMPARISON OF EXISTING AND PROPOSED SYSTEMS

Table 1 Comparison between PLGP and PLGPa (PLGP-Parno_Luk_Gaustad_Perrig)

PLGP	PLGPa
PLGP doesn't have attestation	It is PLGP with attestation
Forwarding nodes doesn't know the path of the packet	Each packet has a verifiable path history
Doesn't hold backtracking	Holds backtracking
Vulnerable to Vampire attacks	Resistant to Vampire attacks

Table 2 categorization of attacks

Attack	Features	Disadvantages of Defences
Sleep Deprivation Torture	Prevents nodes from entering sleep cycle and depletes batteries faster	It considers attacks only at the Medium Access Control (MAC)
Resource Exhaustion	Mentions resource exhaustion at MAC and transport layers	Only offers rate limiting and elimination of insider adversaries
Flood Attack	Multiple request connections to server, run out of resources	Punishes nodes that produce burst traffic but may not send much data
Reduction of Quality of Attacks	Produce long term degradation in networks	Focus is only on transport layer and not on routing protocols
DOS Attacks	Malefactor overwhelms honest nodes with large amounts of data	Applicable only to traditional DOS. Doesn't work with intelligent adversaries i.e., protocol complaint
Wormhole Attack & Directional Antenna Attack	Allows connection between two non-neighbouring malicious nodes : disrupt route discovery	Packer Leashes: Solution comes at high cost and is not always applicable
Minimal Energy Routing	Increase the lifetime of power constrained networks using less energy to transmit and receive packets	Vampire attacks increase energy usage even in minimal energy routing

RESEARCH ARTICLE

7. CONCLUSION

We defined Vampire attacks, a new class of resource consumption attacks that use routing rules of conduct to permanently disable (something made for a particular reason) wireless sensor networks by using up/reducing nodes' battery power. These attacks do not depend on particular rules of conduct or putting into uses, but rather expose weaknesses in some popular rules of conduct classes. We showed some proof-of-concept attacks against representative cases of existing routing rules of behaviour using a small number of weak enemies, and assessed their attack success on a randomly-generated topology of 30 nodes.

REFERENCES

[1] David Marchany, Randy Brownfield, M. Raymond and S. Midkiff, "Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols," in Information Assurance Workshop, 2006 IEEE, West Point, NY, 2006, pp. 297 - 304.

[2] A. Anuba Merlyn and A. Anuja Merlyn, "Energy Efficient Routing (EER) For Reducing Congestion and Time Delay in Wireless Sensor Network", International Journal of Computer Networks and Applications, Volume 1, Issue 1, PP: 1 – 10, November – December (2014).

[3] SARIKA KHATARKAR and RACHANA KAMBLE-Wireless Sensor Network MAC Protocol:SMAC & TMAC(IJCSE:Aug-Sep:2013).

[4] John A.Stankovic Anthony D.Wood, "Denial of Service in Sensor Networks," IEEE, pp. 54-62, October 2002.

[5] Sharon Goldberg, David Xiao, Eran Tromer,Boaz Barak, and Jennifer Rexford,Princeton University (Path-Quality Monitoring in the Presence of Adversaries, June 21-2009.

[6] Richard Han, and Shivakant Mishra Jing Deng, "Defending against Pathbased DoS Attacks in Wireless Sensor Networks," in SASN, 2005, pp. 89-96.

[7] Perrig, A. Yih-Chun Hu and D.B Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003, pp. 1976 - 1986.

[8] Jae-Hwan Chang and Leandros Tassiulas (Energy Conserving Routing in Wireless Ad-hoc Networks).

[9] J.Vijay Daniel, G.Murugaboopathi K.Venkatraman, "Various Attacks in Wireless Sensor Network:Survey," International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 1, pp. 208-211, March 2013.

[10]Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi-Wing Wong On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas (International Journal of Distributed Sensor Networks Volume 2013).

[11]Dr. Shahriar Mohammadi and Hossein Jadidoleslamy-A OMPARISONNETWORKS (International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, March 2011).

[12]TEODOR-GRIGORE LUPU-Main Types of Attacks in Wireless Sensor Networks (Recent Advances in Signals and Systems).

[13]James Newsome, Elaine Shi, Dawn Song and Adrian Perrig -The Sybil Attack in Sensor Networks: Analysis & Defenses(2004 ACM).

[14]Lina r.deshmukh, amol d.potgantwar-prevention of vampire attacks in wsn using routing loop Proceedings of IRF International Conference, 5th & 6th February 2014).

[15]P.Rajipriyadharshini, V.Venkatakrishnan,S.Suganya,A.Masanam-Vampire Attacks Deploying Resources in Wireless Sensor etworks(IJCSIT-2014).

[16]David Xia, Eran Tromery, Boaz Barak, and Jennifer Rexford Sharon Goldberg, "Path-Quality Monitoring in the Presence of Adversaries," in METRICS Measurement and Modeling of Computer Systems, New York, NY, June 2009, pp. 193-204.

[17]D. J. Bernstein. (1996, September) TCP/IP SYN cookies. [Online]. HYPERLINK"http://cr.yp.to/syncookies.html" ,http://cr.yp.to/syncookies.html .

[18]Leo Selavo, and John A. Stankovic Anthony D. Wood, Springer, pp. 531-543, 2008.

[19] Kai Xing , Shyaam Sundhar Rajamadam Srinivasan , Manny Rivera ,Jiang Li , Xiuzhen Cheng (Attacks and Countermeasures in Sensor Networks: A Survey-2005 Springer).

[20]Farzana T, Mrs.Aswathy Babu-A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks (International Journal Of Engineering And Computer Science:Volume 03 Issue 07 July, 2014).

Authors

Ms. Sandhya Rani G received B.Tech from Sri Gnaneswari Research & Technological Academy for Women, and M.Tech from MVGR College of Engineering, (JNTUK affiliated) Andhra Pradesh, India.

Mr. Santosh Naidu P received B.Tech from MVGR College of Engg, and M.Tech from MVGR College of Engineering, (JNTUK affiliated) Andhra Pradesh, India. No. of publications: 7