ISSN:0975-9646

Prevention of battery life depletion from Wireless Ad-Hoc Sensor Networks using Signal Strength

C. Suganthini[1], S. Saranya[2], V.S. Sowmiya[3]

[1] *Assistant Professor,* [2] *Students, Dept of Computer Science and Engineering*
[1 2 3] *Velammal Institute of Technology, Anna University, Chennai, India*

Abstract- In this paper, we discuss some of the threats to wireless ad hoc networks. In wireless ad-hoc networks all communication occurs through a wireless medium. Therefore it probes for a number of security problems. The applications of WSN are rapidly increasing diversely. The routing layer is vulnerable to a kind of DoS attack termed as Resource destroying attacks. Power draining attacks have not been rigorously defined, evaluated, or mitigated at the routing layer so far. These resource destroying attacks are resource consumption attacks which permanently disable networks by draining node's battery power. Resource destroying attacks differ from other DoS attacks by a fact that it do not disrupt immediate availability, but works over time to disable a network. These attacks are not specific to any particular protocol, but depend on the properties of many classes of routing protocols. These resource depleting attacks are difficult to detect as they obey protocol complaint messages and do not alter discovered network paths. We use the signal strength of radio signals in calculating the distance travelled by the packet towards the destination using which power consumption is limited to only the specific nodes that need to participate. Secret key bits are also used to ensure that the appropriate destination is identified.

***Index Terms*— Denial of service, secure routing, ad-hoc networks, sensor networks, wireless networks, resource destroying attacks, signal strength, secret key.**

I. INTRODUCTION

In the networks so far, a secure routing protocol only guarantee the availability of message. Message integrity, authenticity and confidentiality are handled at a higher layer with the help of an end-to-end security mechanism like SSH or SSL. End-to-end security is possible in more conventional networks as it is not necessary for intermediate routers to have access to the content of messages. But in sensor networks, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer and Network layer security mechanisms can help prevent some of the vulnerabilities occurring.

Attackers in a network can be categorized as insider and outsider attackers. An outsider attacker is not an intended user of the network and an insider attacker is an authorized node and a part of the routing mechanism. Routing algorithms are exactly distributed and affect the entire system. It is usual if a malicious outsider cause disrupts to a network. But if an insider node purposely can disrupt the network communications, then there exists certain reasons for its misbehavior. Running out of battery or collisions in the network might cause the node to fail or perform its functionality. The cause for node failure is a serious issue. Such failures can even result preventing some nodes from communicating with other nodes in the network. Malicious adversaries and selfish nodes are those that raise attacks against physical, link, network, and application layer functionality.

To enhance the lifetime of wireless ad hoc sensor networks has become a vital necessity. The usual secure routing protocols tend to identify attacks on the short term availability of a network. But they do not address attacks that affect long-term availability. The most predominant denial of service attack is the resource destroying attacks that entirely deplete the energy of nodes. It is a form of resource exhaustion attack, with battery power as the source of interest. The excessive need of resources has led to a shortage in meeting the needs of the general requirement of the sensor devices. Battery power is the most important resource for sensor networks. Security mechanisms must aim at achieving an efficient communication since the power is expensive. Routing and data forwarding is a crucial service for enabling communication in sensor networks. The current routing protocols suffer from many security vulnerabilities and is not energy efficient. Injection of malicious routing information in the network results in routing insecurities. The wireless medium is less secure that the authentication methods can sometimes fail to find out the adversary activity carried out by the insider adversary.

II. CATEGORIZATION

Resource destroying attacks fall under the category of Denial of Service attacks. They are identified by their incremental change in battery power, processing time, total time taken for transmission etc. DoS attacks in wired networks are usually characterized by amplification. Any malicious insider can amplify the resources it spends on the attack by multiplying its need for resource, e.g. use one minute usage of CPU time causes the victim to use ten minutes. In the process of routing a packet in any multi-hop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached, resources are consumed not only at the source node but also at every node that the message passes through. On taking into account, the cumulative energy of the whole network, attacks amplification of energy usage is always possible, provided an adversary can compose and send messages which are processed by each node along

the message path. Therefore amplification occurs on every attempt to send a message, leading to resource exhaustion, until the aggregate cost of routing a message (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. We must drop this amplification in order to prevent maliciousness and focus on the aggregative energy consumption increase that an adversary can cause while sending the same number of messages as an honest node.

If composition and transmission of a message causes excessive energy to be consumed by the network than that of an honest node transmitting a message of identical size to the same destination, we say that a resource destroying attack prevails. The ratio of the network energy used in the honest case to the energy used in the malicious case, measures the intense of the attack. A ratio of 1 deducts security from resource destroying attacks.

III. Attacks On Wireless Sensor Networks

A. Resource Exhaustion Attacks

A malicious entity can drain network resources by transmitting a large number of data or control packets. The IDS detects this scenario by maintaining a count of the number of packets that it receives from each node within a specific time window. If this count crosses a threshold, then a warning alert is given. This alert signals excessive number of packets. The threshold for control packets is obtained as a function of the number of neighbours that a node have, the rate of HELLO messages, and the rate of retransmission of other control packets.

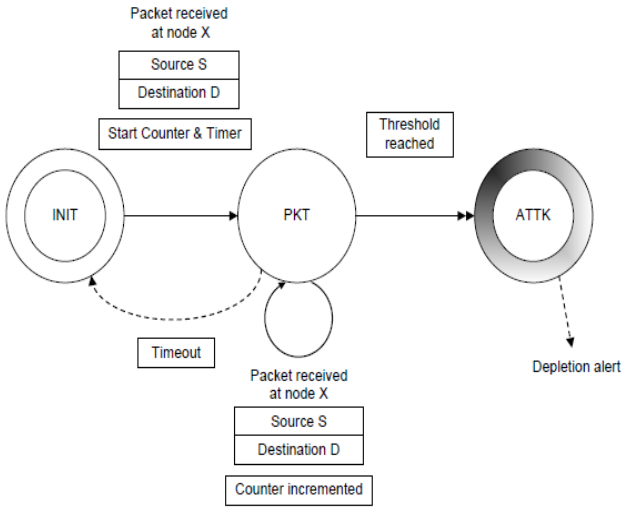


Fig. State Transition Diagram for Resource depletion attack

On sniffing the first packet between the source and the destination, the sensor makes a transition from the initial state (INIT) to an intermediate state (PKT). In this state, both a counter and a timer are initialized. The counter is incremented for every packet the sensor observes between the same source and destination. If the count crosses a threshold within a specific time interval, the sensor moves to ATTK state and raises an alert. The counter is reset if the sensor observes an idle period for a substantial amount of time. A separate counter for the total number of packets sent by each source to multiple destinations is maintained to detect variations of the depletion attack. We consider the elongation attack and its preventive measures to encounter excessive power consumption.

B. Elongation Attack

In the elongation attacks, an adversary constructs artificially extended routes, potentially traversing every node in the network. This is done to increase packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. A malicious insider has number of ways to induce topology change. For instance, it can falsely claim that a link is down or can even claim a new link to a non-existing node.

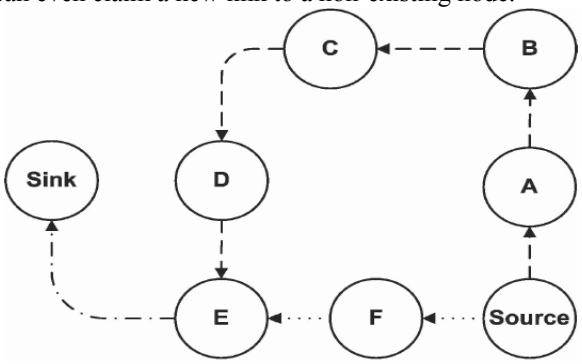


Fig. Elongation attack

This attack is more vulnerable in networks that do not employ authentication or use end-to-end authentication. Here the number of nodes visited is large and equal amount of energy is consumed at each node during traversal. Elongation attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node.

IV. Signal Strength In Attack Prevention

Base Station is simply a wireless access point. The base station in wireless communication is a transceiver connecting a number of devices to another wide area. In computer networks, it is a transceiver acting as a router for computers (nodes) in the network. It is the Base Station Subsystem that handles traffic and signaling, transmission and reception over the air interface. Signal Strength refers to the intensity of the received signal by the Wireless Access Point. A localization technique is used for positioning with access points which is based on measuring RSS (Received Signal Strength). If a distant transmitter is moved closer to a receiver, the strength of the transmitted signal at the receiving antenna will increase. In other words, if the RSS is high it means that the immediate receiving node is nearer and that the extent to which the data can be accessed is greater.

The Received Signal Strength (RSS) value is part of the data packet transmitted. It is intended as means to obtain a relative indication of the quality of connection that exists between the sensor unit and the access point it is

connected to on the wireless network. Here the access point refers to the base station. Signal strength is based on a number of factors, including the output power of the transmitter (the original strength of the signal), the sensitivity of the receiver (how well the receiving device can hear weak signals) the gain of the antennae at both ends of the path, and the path loss, or attenuation of the signal as it travels through the air from the transmitter to the receiver. Signal strength is expressed in units of decibels (dB). RSS can be used internally in a wireless networking card to determine when the amount of radio energy in the channel is below a certain threshold at which point the network card is clear to send (CTS). Once the card is clear to send, a packet of information can be sent. The end-user will likely observe a RSS value when measuring the signal strength of a wireless network.

A. Free Space Path Loss (FSPL)

The distance from the router to destination can be calculated by using the signal strength. Here the router means the every node through which the packet traverses through.

Fade Margin's Equation states that,

$$FSPL\ (dB) = 20\log10\ (d) + 20\log10\ (f) + K$$

$$Distance\ (km) = 10(FSPL - K - 20\log10\ (f))/20$$

Where, d - wireless transmission distance (Km), f - frequency of radio signals (MHz), K – 32.44 (const).

FSPL is the Free Space Path Loss which denotes the probability to which the path can be misguided by an intermediate participating node. The path loss can be due to wrong path discovery, claiming of false path by a deciding node, misdirection by the routing schemes, etc.

B. FSPL from RSS measurements

Free Space Path Loss can be calculated using Fade Margin's equation provided the wireless transmission distance and the frequency of the radio signals are known. In a sensor environment, the RSS can be calculated from the sensor nodes at each point. With this measurement of the signal strength we can calculate the distance between the node that currently has the transmitted data and the destination. This distance can be estimated from the following formula as follows.

Distance = 10 ^ ((27.55 - (20 * log10 (freq)) - RSS)/20)

The distance between the forwarding nodes and the destination is calculated to know whether the packet is forwarded in progress or not. The base station looks after the communication between two ends but still it is necessary to make sure that the data packet does not take an unwanted longer path or a faker one. When a router takes an extended path, it results in draining of battery at unnecessary node points. In order to prevent this occurrence in a dynamic routing procedure, we use the calculated distance to verify the right path traversal. Measuring the strength of the received signals, the quality of the communication can be determined.

The RSS value increases when the receiving point is near or the path is free from obstacles, noise/interference etc. The measurement of the RSS value gives information about how far the data can be accessed or made available.

V. SECRET KEY EXTRACTION

We use a three stage process, comprising quantization, data reconciliation and security amplification, for transforming a set of RSS measurements into secret key bits. The secret key is that which denotes that the node claiming the data packet is the genuine destination of the information. Only upon providing the secret key, will the base station permit the file to be accessed by the other end. The secret key value is a kind of verification that the source does to its destination.

Secret key establishment is a fundamental requirement for private communication between two entities. There is a growing interest in using spatial and temporal variations in wireless link characteristics for extracting secret keys. We investigated the effectiveness of secret key generation using wireless received signal strength in real environments. Public key cryptographic systems are computationally very demanding, which makes such systems unsuitable for resource constrained, battery-powered sensor networks. Therefore, secret key extraction approach that is based on inexpensive measurements of received signal strengths serves as a much better alternative for sensor networks.

A. Quantization

As multiple packets are exchanged between the source and destination, each of them builds a time series of measured RSS. Then, each node quantizes its time series to generate an initial secret bit sequence. The quantization is done based on specified thresholds.

Given a set of RSS measurements, the quantization stage first divides the range of measurements into M equal sized intervals. Then depending on the interval in which a given measurement falls into, $\log_2 M$ bits are extracted from that measurement. Quantization with M=4 intervals is depicted in the figure. The extracted bit sequence is the initially generated input sequence. The same way, a sequence of bits will also be generated at the output.

B. Data Reconciliation

Once the source and destination extract the bit stream from the RSS measurements they collect using quantizers, to agree upon the same key, they must correct the bits where the two bit streams differ. The differences in the two bit streams arise primarily due to the factors like presence of noise or interference, hardware limitations, manufacturing variations, etc. In a wireless environment any transmission is prone to such factors because of changes in external factors. A data reconciliation technique leaks out minimal information to correct those bits that do not match at source and destination. This small amount of information revealed can be in the form of providing keywords or parity bits. By using this technique, the matching of keywords is checked. If the keywords provided by the other end match with those that were given by the source, then the base station allows the destination to retrieve those files that match the keywords. This way helps the base station in identifying that the destination has legal authentication towards receiving the information

transferred from the source. Data reconciliation can also release certain fraction of bits to reconcile the differences in the bit streams of source and destination. All the blocks with mismatching parities are located. Proceeding in a binary search fashion for each such mismatching block, it is checked if a few bits can be changed to make the block match parity. These steps are repeated a number of times with different permutations of the bit streams to ensure a high probability of success.

C. Security Amplification

Security amplification solves the above two problems due to the correlation in bits and the revealed information by reducing the size of output bit stream. This is achieved by letting both source and destination use universal hash functions, chosen at random from a publicly known set of such functions, to obtain fixed size smaller length output from longer input streams. Security amplification addresses both the bit correlation and bit leakage problems by applying 2-universal hash functions on the reconciled bits. This step reduces the length of the output bit stream but at the same time it also increases the per bit entropy (level of bit unpredictability) of the extracted secret key bit stream. This section concentrates on tightening the security by guarding the bit information.

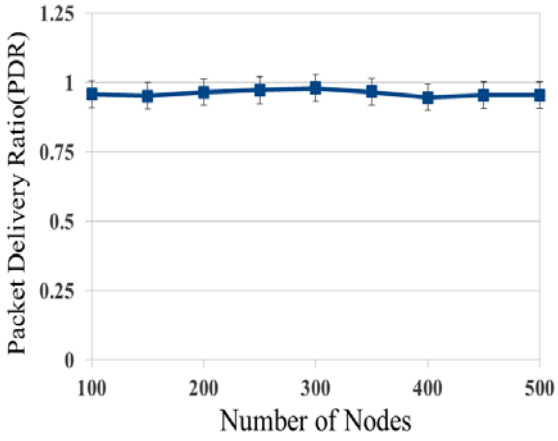
D. Measurement of Energy Usage

Energy usage is measured for the minimum number of packets required to deliver a single message, so sending more messages increases the strength of the attack linearly until bandwidth saturation. We independently computed resource utilization of honest and malicious nodes and found that malicious nodes did not use a disproportionate amount of energy in carrying out the attack. In other words, malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy. Nevertheless, malicious node energy consumption data are omitted for clarity.

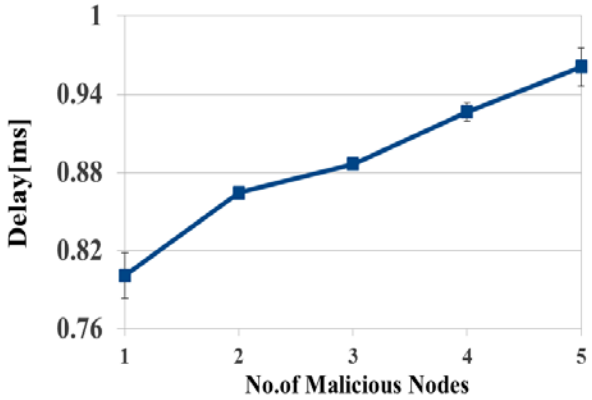
The attacks are carried out by a randomly selected adversary using the least intelligent attack strategy to obtain average expected damage estimates. More intelligent adversaries using strength of their attack by selecting destinations designed to maximize energy usage. More information about the network would be able to increase the energy. The elongation attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. Both attacks significantly increase network-wide energy usage.

VI. PERFORMANCE CONSIDERATIONS

The process of analyzing performance is done by analyzing and measuring the corresponding Delay, Throughput, and Packet Delivery Ratio with range of changing parameters such as speed, packet rate, no. of nodes, no. of connections etc. The graphs drawn with these parameters are used to analyze the performance.



The performance of WSN environment is analyzed with increasing no. of nodes and calculating the Packet Delivery ratio for each of these increasing nodes in sequential order. The above plotted graph depicts the Error Graph that shows the performance under a standard scale that induces 5% of erroneous data in the network.



The above process represents increase of delay over the network as the number of malicious nodes increases. Since the black hole nodes drops the packets that are sent to the destination by acting as intermediate node between both the source and destination. The above approach is carried out over a WSN environment with respect to elongation attack.

VII. CONCLUSION

We showed the mitigation methods for detecting the Resource destroying attacks, a new class of power consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. The characteristics of resource exhaustion attacks make the network more vulnerable such that it cannot be accessed and creates a great damage to users of the Ad-hoc networks like taking the entire network offline. Steps were taken to eliminate such attacks so as to amplify the lifetime of the resources. The received signal strength is ultimately used in all sections. The secret keys finally add up to the security of the transmission. Importance was given mainly to the prediction and detection of these resource draining attacks in the packet forwarding phase.

REFERENCES

[1] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2008.

[2] "Secure routing in wireless sensor networks: attacks and countermeasures" Chris Karlof, David Wagner, University of California at Berkeley, Berkeley, CA 94720, USA, 2003

[3] Abbas Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Network, University Of Sydney", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 2, February 2013.

[4] H. Yih-Chun and A.Perrig. "A survey of secure wireless ad hoc routing", *IEEE Security & Privacy Magazine*, 2(3):28–39, May/June 2004.

[5] "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks" Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, Richard A. Kemmerer, Department of Computer Science, University of California, Santa Barbara

[6] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", IEEE Transactions on Mobile Computing, Vol.12, No.2, pp.1-15, Year 2013.

[7] S. Djahel, F. Naït-Abdesselam and Z. Zhang, ―"Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges", IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 658–672, Fourth Quarter 2011.

[8] Sevil Sen, John A. Clark, and Juan E. Tapiador, ―"Power-Aware Intrusion Detection in Mobile Ad Hoc Networks", Elsevier, pp.1-16, 2010.

[9] Khalil, S. Bagchi, C. Nina-Rotaru, and N. Shroff, ―"UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks", Ad Hoc Networks, vol. 8, no. 2, pp. 148-164, 2010.

[10] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys and Tutorials, Vol.PP, No.99,pp. 1-20, March 2013.

[11] Ashraf Hussain Farooqi, FarrukhAslamKhan, Jin Wang and Sungyoung Lee, " A novel intrusion detection framework for wireless sensor networks", Journals of Springer-Pers Ubiquit Comput, pp.1-13, February 2012.

[12] "A Security Approach for Detection and Elimination of Resource Depletion Attack in Wireless Sensor Network", Ambili M A, Mr. Biju Balakrishnan, Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore

[13] I. Stamouli. "Real time intrusion detection for ad hoc networks", Master's thesis, University of Dublin, September 2003.

[14] Secret Key Extraction in MIMO-like Sensor Networks Using Wireless Signal Strength by Sriram Nandha Premnath, Academic Advisors: Sneha K. Kasera, Neal Patwari,
University of Utah, 2013.