RESEARCH ARTICLE OPEN ACCESS

An Optimized Approach for Attack Detection and Prevention in Wireless Sensor Networks

Vishal Kumar [1], Shaveta Jain [2]
Assistant Professor [2]
GGS College of Modern Technology
Kharar (Mohali)
India

ABSTRACT

The WSNs are designed of several "nodes" – from a small to large or even very large, wherever every node is connected to one sensor. The sensor network node contains completely different parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for sensor activity and an energy supply, usually electric battery or an embedded form of energy harvesting. The size of Wireless Sensor Network can vary from large too small. The different topologies are present for WSN like bus topology, star topology and fully connected mesh topology. Whenever Communication or routing happens there’s threat of false reports and wormhole attacks in WSN. Thus a secure routing methodology is used for detecting false report injections and wormhole attacks in wireless sensor networks.

Keywords: - Wireless sensor network, Wormhole attack, Black hole attack & Denial of service attack, nodes, routing methodologies.

I. INTRODUCTION

Wireless Sensor network is an emerging technology that provides a new paradigm for computation and communication. It consists of large number of autonomous sensing devices that are responsible for monitoring the physical and/or environmental conditions such as temperature, humidity, sound, pressure, motion, vibration, pollution etc. of a target area. Data collected by these sensing devices are transmitted to the destination called sink or base station. Usually, the base station has higher computation and communication capability. Sensing devices co-ordinate among themselves to carry out a given task. These networks are bidirectional in nature for controlling the network from both sides. In the early time the Wireless Sensor network are used and by the military services but now today these networks are used by various industries and consumer applications for health monitoring, industrial process monitoring, natural disaster prevention and water quality monitoring etc. WSNs are currently used for real-world unattended physical environments to measure numerous parameters. Therefore, the characteristics of a WSN must be considered for efficient deployment of a network. The main characteristics of a WSN includes (i) Communication Capability: a WSN typically uses radio waves over communicational channel. It has the property of communicating in short range, with limited and dynamic bandwidth. The communication channel can be bidirectional and unidirectional.

(ii) Computational Power: normally a node in a WSN has limited computational capabilities as the cost and energy need to be considered. (iii) Security and privacy: Each sensor node ought to have adequate security mechanisms so as to stop unauthorized access, attacks, and unintentional damage of the information within the sensor node.

(iv) Distributed sensing and processing: the several sensor nodes are distributed uniformly or randomly. In WSNs, every node is capable of collecting, sorting, processing, aggregating and sending the information to the sink. Thus the distributed sensing provides the robustness of the system.

(v) Dynamic network topology: normally WSNs are dynamic networks. The sensor node can fail for battery exhaustion or other circumstances. Communication channel can be distorted as well as the additional sensor node may be added to the network. All those, result in frequent changes for the network topology.

(vi) Self-organization: the sensor nodes in a network must have also the ability of organizing themselves as the sensor nodes are deployed in a unknown fashion in an unattended and hostile environment. The sensor nodes have to work in collaboration to adjust themselves to the distributed algorithm and form a network automatically. **Platforms** of wireless sensor network includes:

(i) **Hardware:** in a WSN normally large number of sensor nodes are placed to measure the desired physical environment. In order to reduce the total cost of the complete network the cost of the sensor node must be kept as low as possible. In many applications, a WSN communicates with a Local Area Network with the help of gateway. The gateway acts as a bridge between the WSN and the other network. This allows data to be stored and processed by devices with additional resources, for example in a remotely located server.

(ii)**Software**: energy in WSNs is used for different purpose such as computation, communication and storage. Sensor nodes consume more energy compared to any other for communication. If they run out of the power they often become invalid as it does not have any option to recharge. For this reason, algorithms and protocols need to address the issues such as lifespan is increased, and make the system robustness and fault tolerance and self configuration.

(iii)**Operating System:** the operating system used in wireless sensor networks is less complex as compared to the general purpose operating system. Because wireless sensor networks are typically deployed with a particular application and there is also no need of virtual memory for low cost and low power microcontroller. It is therefore suggested to use newly developed operating systems such as Riot, Contiki, Lite OS. The first operating system used in the wireless sensor network is TinyOS and it is based on event-driven programming model instead of multithreading. The programs of this operating system are composed of event handler and tasks with run-to-completion semantics.

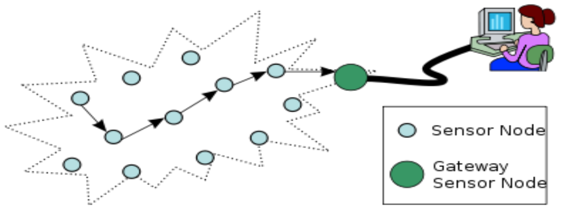

Figure 1: Typical multi-hop wireless sensor network architecture

A. *Routing*

The term "*routing*" is usually employed for taking a packet from one device and sending it through the network to another device on a different network. The method of routing chooses the most effective path in the network for the transmission. Routing is also known as forwarding. The Routing is performed by different types of networks like telephone network, electronic data networks and transportation network. In packet switching networks the entire message is broken down into smaller packets and switching information is added in header of each packet. The transmission is done through the intermediate nodes. Intermediate nodes are usually network hardware devices such as routers, bridges, gateways, firewalls or switches. The routing process follows the routing table which contains different routes for forwarding packets to destination. So the routing table is constructing and kept in the main memory for efficient routing. Most routing algorithms use at most one network path at a single time. Multipath routing techniques allows the use of multiple possible paths. The number of elements are considered in order to decide which routes get installed into the routing table on the basis of priority in the case of overlapping of different routes.

(i)Prefix length: Where longer subnet masks are preferred.

(ii) Metric: Where a lower metric is preferred.

(iii) Administrative distance: Where a route learned from a more reliable routing protocol is preferred.

Routing schemes differ in their delivery linguistic:

- Unicast delivers a message to one specific node.
- Broadcast delivers a message to all or any node within the network.
- Multicast delivers a message to a batch of nodes that indicates interest in receiving the message.
- Anycast delivers a message to anyone out of a batch of nodes, usually the one closest to the source.
- Geocast delivers a message to a geographical region.

B. *Topology Distribution*

In static routing, small networks may use manually configured routing tables. Larger networks have compound topologies which changes rapidly, making the manual construction of routing tables inconvenient. Nevertheless, if the direct route becomes blocked, most of the general public switched telephone network uses pre-computed routing tables with fallback routes.

Adaptive routing is used to solve this problem by automatically constructing routing tables, accordance with the information carried by routing protocols, allowing the network acts as avoiding network failures and blockages.

There are number of algorithms which used for routing such as

(i) Distance vector algorithm : This method assigns a cost number to each of the links between each node within the network. The lowest total cost path will always be chooses by the nodes in the network for sending the message. This algorithm operates in a very simple manner. When a first or primary node in the network starts, it only have knowledge of its immediate neighbors, and the overall cost involved in reaching them. Every node on a regular basis, sends to every neighbor node its own current assessment of the entire cost to get to all the destinations it knows of. The neighbor node examine this data and compare it to what they already know. Over time all the nodes within the network can discover the most effective path with low cost. When one network goes down, any nodes that used it as their next hop discard the entry, and make new routing-table data. These nodes send the updated routing information to all adjacent nodes, and the nodes within the network receive the updates and find out new paths to all the destinations.

(ii) Link State Algorithm: By applying link state algorithm, a graphical map of the network is the fundamental data for every node. To produce its map every node floods the whole network with information about the other nodes it can connect to. Each node independently places this data into a map, every router independently find out the low-cost path from itself to every other node by using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is in form of tree graph rooted at the current node, such that the path through the tree to any other node is the low cost path for that node. This tree now serves to built the routing table, which specifies the most effective hop to get from the current node to any other different node.

(iii) Optimised Link state routing algorithm: This is often optimised for ad hoc networks. It uses hello and also topology control messages to find out the link state information with the mobile ad hoc network. Using hello messages, every node discovers 2-hop neighbor information and selects a group of multipoint relays.

(iv) Path Selection: This includes to applying a route metric to multiple routes, so as to find out the most effective route.

In computer networking, the metric is determined by a routing algorithm, and includes information such as bandwidth, hop count, path cost, load, network delay, reliability and communication cost. The routing tables stores only the most effective routes, while link state also store information. Because a routing metric is particular to a given routing protocol, multi protocol router should use some external heuristic in order to select routes from different routing protocols. In local network administrator, in particular cases can set up host specific routes to a specific device that provides additional control over network usage, permits testing and overall better security. This may available in handy when debugging network connections. In small systems the central single device decides the path of each packet. In another small system, wherever edge device insert a packet into the network decides ahead of the time complete path of that particular packet. In both types of system, the route planning device requires information about the devices which are connected to each other. If it has this information, it may find the most effective path by using A* search algorithm.

C. Attacks On Wireless Sensor Network

In several applications the information obtained by the sensing nodes must keep confidential and it's to be authentic. In the absence of security, a false or malicious node might intercept non-public information, or might send false message to nodes within the network. Wireless sensor network are exposed to security attacks due to the broadcast nature of the transmission medium. Moreover wireless sensor networks have a further vulnerability because nodes are usually placed in a hostile or dangerous environment wherever they're physically protected.

Types of Attacks are:

- The Wormhole Attacks
- Black Hole Attacks
- Denial Of Service Attack

Wormhole Attack: One node within the network sends a message to a different node within the network. Then the receiving node tries to send the message to its neighbor. The neighboring nodes suppose the message was sent from the sender node so this node tries to send the message to the originating node, but due to large distance it never arrives. Wormhole attack could be a vital threat to wireless sensor network as a result of this type of attack doesn't need compromising a device within the network, rather it can be performed even at the initial part once the sensors begin to get neighboring information. These attacks are hard to counter because information provided by the node is hard to verify.

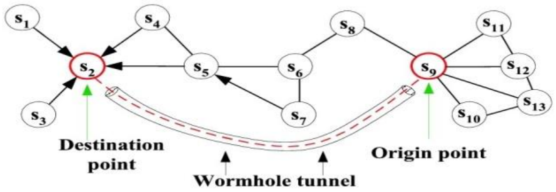

Figure 2 : Wormhole Attack

Black Hole Attack: Black Hole Attack: It's sort of denial of service attack within which a router that is assumed to reply packets instead discards them. This typically happens from a router becoming compromised from a number of varieties of causes. One cause mentioned in research is through a denial of service attack on the router employing a known DoS tool. Because packets are often dropped from a lossy network, the packet drop attack is very difficult to observe and stop. The malicious router can even accomplish this attack by selection, eg by dropping packets for a selected network destination, at a particular time of the day, each n packets or each t seconds, or a arbitrarily selected portion of the packets. This is often referred to as grey hole attack. If the malicious router attempts to drop all packets that are available in, the attack will be really discovered quickly through common networking tools such as tree route. Also, once alternative routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router form their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a selected time period or over each n packet, it is usually difficult to detect because one traffic still flows across the network.

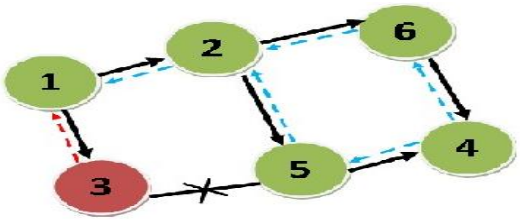

Figure 3 : Black Hole Attack

In shown figure an RREQ broadcast from node 1 is received by neighboring nodes 2,4 and 5. However, malicious node 5 sends an RREP message instantly without even having a route to destination node 3. The RREP massage sent by the malicious attacker node is the initial message reaches to the supply node. When the supply node receive the message sent by the malicious attacker node, updates its routing table for th**e** new route for the meant destination node and then also rejects any other RREP message from other neighboring nodes even from an actual destination node. When the supply node receive the route, it sends the data packets instantly from the route which is supplied by the malicious attacker node, a black hole node 3 drops all data packets instead of forwarding them.

II. LITERATURE SURVEY

Min-kyu Choi (July, 2008) "Wireless Network Security: vulnerability Threats and Countermeasures" Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization's overall information security risk profile. Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities, wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. We present a framework to help managers understand and assess the various threats associated with the use of wireless technology. We also discuss a number of available solutions for countering those threats.

Nidhi Chhajed Nov 2014 "Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review" Wireless Sensor Network is one of the emerging areas of research in present scenario. It is a wireless means of communication in which nodes can communicate without any physical medium. As there is no communication media, the data is transmitted from one node to another in the form of packets. Thus, it is easy to capture packets by the unauthorized users. Various types of attacks can be applied in the sensor networks by compromising legitimate nodes, by inserting malicious nodes and many more in a network in order to access the information which is the most important thing. Among various attacks like Sybil attack, wormhole attack, sinkhole, flood attack, selective forwarding attack, black hole attack, etc black hole attack has been an important research area for a long period of time. In this review, our main focus will be on the detection and prevention techniques for black hole attack in WSNs.

Ateeq Ahmad "Type of Security Threats and It's Prevention" Security is a branch of computer technology known as information security as applied to computers and networks. The objective of online security includes protection of information and property from theft, corruption, or threats attack, while allowing the information and property to remain accessible and productive to its intended users. The term online system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The basic aim of this article is to Prevention against unauthorized security Attack and Threats.

G.Mahalakshmi Feb 2014 "A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks" Wireless sensor network is vulnerable to various attacks due to the deployment in hostile environment. Among various types of security threats, low power sensor nodes are affected by the attacks that cause random drainage of the energy level of sensors. It leads to the death of nodes. The denial of sleep attack is the most dangerous type of attack in this category. Most of the existing approaches to detect denial of sleep attack involve lot of overhead, which lead to poor throughput. In this survey, different approaches for the detection and prevention of denial of sleep attacks in wireless sensor networks are described.

Umesh Kumar (2014) "A Literature Review of Security Threats to Wireless **Networks"** In the recent years we have huge development of wireless technology. We are presently getting more subject to wireless technology. As we know wireless networks have broadcast nature so there are different security issues in the wireless communication. The security conventions intended for the wired systems can't be extrapolated to wireless systems. Hackers and intruders can make utilization of the loopholes of the wireless communication. In this paper we will mull over the different remote security dangers to wireless systems and conventions at present accessible like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is more hearty security convention as compared with WPA on the grounds that it utilizes the Advanced Encryption Standard (AES) encryption. There are few issues in WPA2 like it is helpless against brute force attack and MIC bits could be utilized by programmer to compare it with the decoded content. So in this paper we will concentrate on different sorts of wireless security dangers.

Priya Maidamwar (October, 2012) "A Survey On Security Issues To Detect Wormhole Attack In Wireless Sensor Network" Sensor nodes, when deployed to form Wireless sensor network operating under control of central authority i.e. Base station are capable of exhibiting interesting applications due to their ability to be deployed ubiquitously in hostile & pervasive environments. But due to same reason security is becoming a major concern for these networks. Wireless sensor networks are vulnerable against various types of external and internal attacks being limited by computation resources, smaller memory capacity, limited battery life, processing power & lack of tamper resistant packaging. This survey paper is an attempt to analyze threats to Wireless sensor networks and to report various research efforts in studying variety of routing attacks which target the network layer. Particularly devastating attack is Wormhole attack- a Denial Service attack, where link between two points in the network. With focus on survey of existing methods of detecting Wormhole attacks, researchers are for researchers are in process to identify and demarcate the key research challenges for detection of Wormhole attacks in network layer.

C. Sreedhar (2010) "A Survey on Security Issues in Wireless Ad hoc Network Routing Protocols" An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. Due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and non repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. In this paper we attempt to analyze threats faced by the ad hoc network environment and provide a classification of the various security mechanisms.

Sahabul Alam (April, 2014) "ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK" Wireless Sensor Network(WSN) is an emerging technology and explored field of researchers worldwide in the past few years, so does the need for effective security mechanisms. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats due to unattended installation of sensor nodes as sensor network may interact with sensitive data and /or operate in hostile unattended environments. These security concerns be addressed from the beginning of the system design. The intent of this paper is to investigate the security related issues in wireless sensor networks. In this paper we have explored general security threats in wireless sensor network.

III. PROBLEM FORMULATION

The security of nodes while selecting a route for data selection is one of the main issue in wireless networks. Security plays an important role for the system to be reliable and efficient. In the earlier techniques that ensure security of the route selected for the transmission of data the emphasis was laid on the reputation of the nodes. In these conventional techniques first the reputation of the nodes was checked and the selection of the route is done. After the selection of the route the reputation of the each node is updated after each route selection that made the system cumbersome. A new technique is to be Introduced that can efficiently select the route so that high security to the nodes is provided and the data can be reliably transmitted from the source node to the destination node.

IV. PROPOSED WORK

In the proposed technique the security of the system is enhanced by changing the criterion for route selection. In the earlier techniques only the reputation of nodes was considered for route selection but in this proposed technique certain quality of service parameters are also considered along with the reputation of nodes. The factors that are to be considered for route selection are:

- Trustworthiness of node
- Packet delivery ratio
- Throughput

The reputation of the nodes will be checked and then an area will be defined along with that the genetic algorithm for route selection will be used to get the optimized solution of node selection in the route form source to destination which will be attack free.

V. CONCLUSION

In this paper wireless sensor network are discussed in regard to the transmission of data that is the routing techniques which are used and during the transmission of data there are various kind of attacks such as black hole and wormhole attacks which result in data or information loss so as to detect false reports and attack injection a secure routing method is used to securely transmit the data.

REFERENCES

[1].Nidhi Chhajed Nov 2014 "Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review"

[2].Dines Kumar.V.S Jan-Mar 2014 "Protection against Denial of Service (Dos) Attacks in Wireless Sensor Networks"

[3].G.Mahalakshmi Feb 2014 "A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks"

[4].Umesh Kumar (2014) "A Literature Review of Security Threats to Wireless Networks" International Journal of Future Generation Communication and Networking Vol.7, No.4 (2014), pp.25-34

[5].Jyoti Thalor February 2013 "Wormhole Attack Detection and Prevention Techniques in Mobile Ad Hoc Networks: A Review"

[6].Ateeq Ahmad "Types of Security Threats and It's Prevention" Int.J.Computer Technology & Application, Vol 3 Issue 2, pp 750-752

ABOUT AUTHORS

Vishal Kumar obtained B.Tech degree in Computer Science & Engineering (CSE) in 2013 from Ferozepur College of engineering & Technology, Ferozepur, Punjab. He is currently pursuing M.Tech degree in Computer Science & Engineering from GGS Collegee of Modern Technology, Kharar, Punjab. His research area are routing process and security in wireless sensor network.

Shaveta Jain received her B.Tech degree in Information Technology from Global College of Engineering & Technology, Khanpur Khui, Punjab, India in 2012, the M.Tech degree in Computer

Science & Engineering from Maharishi Markandeshwar University, Mullana, Haryana, India, in 2014. She is working as Assistant Professor in Department of Computer Engineering, in GGS College of Modern Technology Kharar Chandigarh. Her research interests include Mobile Ad-hoc Networks.