ISSN:0975-9646

Intrusion Detection and Prevention in Homogenous Wireless Sensor Networks

Vanita B. Raut

Department of Computer Engineering,
G.H.R.I.E.T, Savitribai Phule Pune University
India, Pune

***Abstract*— Wireless Sensor Networks (WSNs) are used for the applications like military, health-related, ecological area. These applications include monitoring of sensitive information such as enemy movement at battlefield, or the location of personnel in the building. Wireless sensor nodes sense around them and detect anomaly event in the industrial environment. For the industrial application it is difficult to detect the intrusion on wireless medium. Intrusion Detection is most essential requirement for security purpose. Security issues are discussed and apply the security algorithm on the nodes. The proposed work to improve security of clustering based network throughput, packet delivery ratio, and it optimizes energy. In this project throughput was increased at Gate Way (GW) and Common Node (CN). Packet Delivery Ratio was increased at GW and CN. Delay was Decrease and Energy consumption was done. Constructed Black Hole attack detection algorithm in hierarchical frame work for intrusion detection.**

***Keywords*— Ad-hoc network, Wireless Sensor Network (WSN), Attacks, ,Intrusion Detection, Intrusion Prevention, zigbee, black hole attack**

I. INTRODUCTION

A WSNs consists of autonomous sensors to monitor physical or environmental sensors. WSNs is made up of hundreds even thousands of small sensor networks [1][2]. After sensor nodes are deployed they automatically route and sense surrounding and automatically compute and transmit the sensed data to the base station (BS) [1]. Because the sensor nodes have limited energy, So in WSN energy consumption is required. For that purpose clustering based routing protocol is used for WSN to save energy. WSN are used for data collection and processing in real time environment. The required Conditions are measured by sensors and then measurements are processed in order to assed situation accurately in area around the sensors. In a large geographical area large numbers of Sensor nodes are deployed accurate. There are two types of WSN one is unstructured and other is structured. The Structured WSN are the sensor nodes which are deployed in a planned manner. Whereas unstructured WSN are the one in which sensor nodes deployment is in ad-hoc manner. There is no fixed basic structure and facility between WSN for communication.

In WSNs attacks can be categorized according to the security requirements in WSNs: Attacks on network availability that is DOS attack, Stealthy attacks against service integrity, Attacks on secrecy and authentication.

A. Motivation

WSNs and are new communication mobile ad hoc networks (MANETs) paradigms. MANETs do not require wired infrastructure or expensive base stations. Nodes can communicate each other directly within radio range and those which are apart use other nodes as relays. Each host in the MANET acts as a router. The routers are mostly multi-hop. In micro electro mechanical systems (MEMS) and wireless communications had made it feasible to built miniature wireless sensor nodes and that data processing, integrate sensing and communicating capabilities.

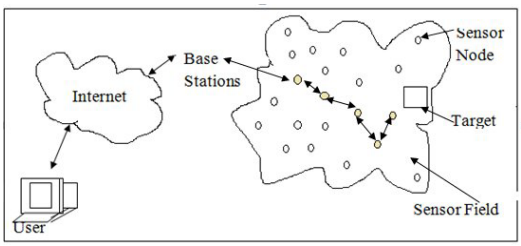

Fig 1: Wireless Sensor Network.

The WSN is implemented in the figure. The WSN is deploying to sense the target [6]. The collaboratively route the data to a base station for analysis. After analysis the base station can transmit the data further to users through another communications route (e.g. internet).

The security solutions for WSNs have originated from the prevention point of view. In the WSNs many key distribution schemes can be built based on link layer security architecture, prevention of DOS attacks, and secure routing protocol. The most important purpose of deploying WSNs is to collect relevant data. The WSN system should be:

1. Fault tolerant: The system should be robust against node failure (running out of energy, physical destruction, H/W, S/W issues etc). Some mechanism should be incorporated to indicate that the node is not functioning properly.

2. Scalable: The system should support large number of sensor nodes to cater for different applications.

*3. Long life***:** The nodes life-time entirely defines the networks life-time and it should be high enough. The sensor node should be power efficient against the limited power resource that it have since it is difficult to replace or recharge thousands of nodes.

4. Programmable: the reprogramming of sensor nodes in the field should ht be necessary to improve flexibility.

5. Secure: The node should support the following:

a] Access Control: to prevent unauthorized attempts to access the node.

b] Message Integrity: to detect and prevent unauthorized changes to the message.

c] Confidentiality: to assure that sensor node should encrypt messages so only those nodes would listen who have the secret key.

*6. Affordable***:** the system should use low cost devices since the network comprises of thousand of sensor nodes, tags and apparatus. Installation and maintenance of system elements should also be significantly low to make its deployment realistic.

B. ZigBee Sensor

Zigbee is the set of specs built in the region of the IEEE 802.15.4 wireless protocol. Zigbee is designed to provide highly efficient connectivity between small packet devices. This sensor supports the symmetric key encryption [1] using Cipher Block Chaining (CBC) security protocols are used as basic security mechanisms and authentication using Message

Authentication Code (MAC). The Zigbee is designed for a low cost, flexible and standard-based wireless network technology, which requires low power consumption, interoperability, reliability, and security for control and monitoring the applications. Zigbee support the Advanced Encryption Standard (AES) with 128 bit data and key integrity using MAC. In zigbee all sensor nodes share one secret key and the whole network can be cooperated if an attacker reached.

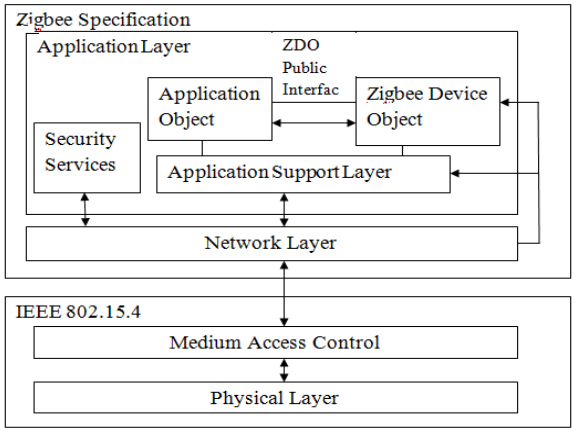

Fig 2. Zigbee sensor

II. Literature Survey

A. An Intrusion Detection and Prevention

The two level hierarchy of the framework [1], in this paper author use the intrusion prevention protocol and intrusion detection protocol. In this method they give the security to every node. In this they can use the one hop and two hop strategies. In this strategies if a node is misbehaves means that node drops the packets.

Hierarchical intrusion detection protocol: In hierarchical based intrusion detection method data is flow from lower to higher level. Gateway (GW), Cluster Head (CH), Member Node (MN) these nodes have two basic attributes data aggregation and event sensing. Member node (MN) delivers the data to the cluster head and cluster head (CH) sends it to the gateway (GW). Each node has IDS module. IDS module contains ID rules and ID handling techniques. If the condition of rules in the module of intrusion detection is satisfied then the sensor node concludes that the malicious intrusion occurs. Using that intrusion can be detected. After detection prevention can be taken for that Localized Encryption and Authentication protocol (LEAP) is suitable.

Advantages:

- Security to the WSN applications
- Detect malicious node
- Performance of packet transmission increase.

Disadvantages:

- The System is not useful for heterogeneous network
- Energy consumption is done
- Unnecessary Traffic generated at CH and GW

B. Energy Efficient Hierarchical Clustering Algorithm for WSN

The wireless network consists of a large number of small sensors which having low power transceivers for gathering a data in a different environments [4]. The data collected by each sensors is communicated through the network to a single processing center that uses all reported data to detect the data. Clustering sensors are in group so that they can send information to the cluster head or they can communicate to the cluster head. The cluster head sends the aggregated information to the processing center. In this paper they extend the Energy Efficient algorithm to organize the sensors in a wireless sensor network into clusters. Energy Efficient, Single Level Clustering Algorithm.

Advantages:

- Energy Optimization done
- Contention free environment
- This is suitable for large number of nodes

Disadvantages:

- It require large number of keys

C. Intrusion prevention and detection approaches for clustering based sensor networks

In this paper they are using two approaches to improve the security of clustering based sensor networks [2]

1. Authentication Based intrusion Prevention
2. Energy Saving or intrusion detection.

Different types of mechanism are also need to monitor cluster heads and member nodes according to the importance of them. When monitoring CH that is cluster heads member nodes of these cluster head take turns to monitor this cluster head. This mechanism reduce time, so that it saves energy of member node, cluster head have mechanism to change the property.

Clustering based routing protocol (CBRP) is important protocol for WSN to save the node energy. It is a routing protocol proposed for WSN to save node energy. At regular intervals, a set of cluster heads is selected and the other sensor nodes that are member nodes are clustered with cluster head according to the clustering algorithm. WSN is deployed in the battle field for museum surveillance, military purposes, or in hospital for monitoring patient

condition, here secure data delivery is required. The unsecure data delivery damages the security of applications. The security in CBRP is distinctive from others because CHs demands security assurance than the sensor nodes. The generic approaches are proposed to secure clustering-based sensor network (CBSN). The planned intrusion detection approach understands the compromised nodes within a threshold in a local cluster. The nodes including cluster head and member nodes which are identical in the initial energy, communication power, storage and the unlimited energy. The base station has powerful computation power, unlimited energy and storage. When sensor node is deployed it fixes its location. In WSN packets are classified in to two types that is control message and sensed data. In this paper time key chains are used.

Advantages:

- Energy optimization is done
- Detection of attacks
- Prevention on them
- Increase packet delivery ratio

Disadvantages:

- The network lifetime is extended when WSN is under attack.
- Sensor nodes cannot move and you cannot add new sensor node.

C. *Intrusion Detection Techniques In Mobile Ad-hoc and WSN*

Mobile ad-hoc networks and WSN have wide variety applications. They cannot be readily deployed without first addressing security challenges. Intrusion detection provide necessary layer of in detail security in wired location. The mobile Ad-hoc networks (MANET) and WSN are the two communication paradigms. MANET do not require wired infrastructure or expensive base stations. Within radio range nodes can communicate directly over wireless links, and the nodes which are out of radio range they can use other nodes as relays. Routers are multi hop that's why each host in the MANET acts as router. MANET could be deployed quickly in scenarios such as meeting room, fire fighting, and city transportation wireless networks and so on. To form a cooperative network every mobile node should be friendly node and willing to send the messages to others.

D. *Decentralized intrusion detection in wireless sensor networks*

- *Data repetation attack and delay*

The detection of the delay a is directly related to the buffer sizes. If buffer size was small the IDS receives the delayed message at the beginning of the buffer more often [5].

- *Data Alteration*

The effectiveness and the number of false positives for this attack. The data alteration attack is confused with data alteration occasional failures. There can be observed a tradeoff between detection effectiveness and the number of false positives.

- *Jamming*

The jamming attack can be confused with the message collision occasional failure. It is one of the attacks with better detection results. The number of false positives is low, similar to the results obtained from the data alteration attack simulation. Like the attacks confused with message loss, detection levels were proportional to buffer levels.

- *An intrusion detection system for wireless sensor networks*

Different routing, medium-access and distributed control algorithms used for detection The wireless channel does not change during the transmission of a whole packet, however, it is random and independent from packet to packet [7].

A model for distributed intrusion detection in sensor networks which is designed to work with only partial and localized information available at each node of the network. Nodes collaborate and exchange this information with their neighbors in order to make a correct decision on whether an attack has been launched. How IDS system can be used to detect black hole and selective forwarding attacks, producing very low false-negative and false-positive rates.

E. *Detecting Misbehaving Nodes in MANETs*

In this paper they proposed IDS scheme designed for MANET. In this each node in network require both transmitter and receiver [6]. MANETs are two types, single hop and multi hop. For single hop network nodes are free to directly communicate with other node that is out of its radio range. In multi hop nodes are communicate out of its own radio range. The cooperation of the node in the network is needed. Node blives on other node to send the packets. In this paper they study the watchdog attack and parthrater attack.

Advantages

The watchdog is capable of detecting misbehavior at the forwarding level instead of just on link level.

Disadvantages

It may fail to detect a misbehaving node in the presence of a) ambiguous collisions b) receiver collision c) Limited transmission power d) false misbehavior report e) collusion f) partial dropping

F. *An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks*

If in network there were no malicious node at that time packet delivery ratio for each scheme were all at 100%. However, when the percentage of malicious nodes increased to 10%, sender sends message to the second node through other node at that time that second node or receiver send acknowledgement to the sent node is called Two acknowledgement (TWOACK), After Multiple number of nodes acknowledgement send to the sender from receiver called AACK and Enhanced Adaptive Acknowledgment (EAACK) outperformed Watchdog scheme. And the delivery ratio of the proposed scheme EAACK toped at this scenario. This is because the introduction of MRA scheme improved the detection performance and thus delivered more packets than all the other competitors. However, the PDR of EAACK turned out to be slightly lower than AACK and TWOACK when the malicious nodes reached. This is likely due to the fact that almost half the nodes in the network are malicious; it's much harder for the source node to find another valid route to the destination node to carry on the MRA scheme.

Advantages:

- Provide Security to the data
- Prevention from attacks

Disadvantages:

- Each node send and receive acknowledgement
- It consumes Time
- It consumes Energy
- Delivery ratio decrease when node malicious

III. System Information

By implementing hierarchical framework and considering intrusion detection and data processing and construct hierarchical intrusion detection and prevention protocol.

A. *Intrusion Detection and prevention*

In this paper we have constructed hierarchical network on the basis of two level clustering. taking logical protocols in this hierarchical framework; an intrusion detection and intrusion prevention protocol. WISNs should be robust and self-repairing. For satisfying these requirements, every sensor node in detection protocol estimates intrusions by itself using its IDS module and handles them by using a gateway and cluster head. In WSN real-time, reliable Communication was considered. The detection protocol with the hierarchical framework enables WSNs to serve a timely and reliable warning on their industrial applications and systems. In the hierarchical intrusion prevention protocol, it is feasible to transmit sensing and detecting results in a timely and reliable manner through in-network processing and prevention mechanisms such as encryption and message authentication codes, respectively. Besides, both detection techniques and symmetric cryptography algorithms adopted for intrusion detection and prevention spend less time for executing them. Thus, our protocols may satisfy the typical requirements.

a) Event Sensing Data Aggregation

A MN delivers the sensed data to its higher level or to the cluster head (CH). Each GW and CH collect and process the data delivered from the lower levels (CHs or MNs, respectively) and then transmit it to a higher level it may be Gateway or the base station (the BS or GW, respectively).

b) IDS Module

Each node also has a IDS module. IDS module has two sub modules:

- *Intrusion Detection Rules:* that decides an intrusion through applying detection rules and threshold to the neighbor's traffic
- *Intruder Handling:* The work of intruder is to handles the intrusion. Each industrial application can employ different detection techniques to the module of intrusion detection rules according to its security requirements.

c) Intrusion Prevention Based on Two-Level Clustering

Intrusion detection within each level and between levels operates by eavesdropping traffic one-hop, and by evaluating the transmitted control and sensing messages. As we mentioned, two-level clustering generates four levels: base station (BS), gateway (GW), cluster head (CH) and member node (MN). Eeach level detects intrusions with the similar detection rules, each level performs a different handling method.

B. *Algorithm:*

Step 1. Shortest Path Algorithm

1.Take the inpute as nodes and arrenge it hierarchical manner calculate CH Cluster Head= (No. Of Nodes* 10/100)

2.Remaining nodes are common nodes.

Step 2. Secure Key Algorithm

1.Sent data through common node sent and receive packet both are set 1, Keys are generated Randomly. At the time of sending packets Use the secret Key for Encryption.

2. After receiving by receiver decrypt the same data using Decryption. In this case Sender and receiver must have the same key.

3. Repeat same for CH and GW.

IV. Experimental Results

Figure 3 shows the scenario of hierarchical topology in this scenario 0 represents the sink node, 1 represents the Gate Way, 2,3,4,5,6 are the cluster Heads. Others are the common nodes. Blue common nodes have cluster head 2. Meaning of this is common nodes have to send data to the cluster head. Red Clusters having node 3 as a cluster head. Dark green clusters have node 4 as a cluster head. Green nodes have cluster head 5. Blue cluster heads have 6 as cluster head.

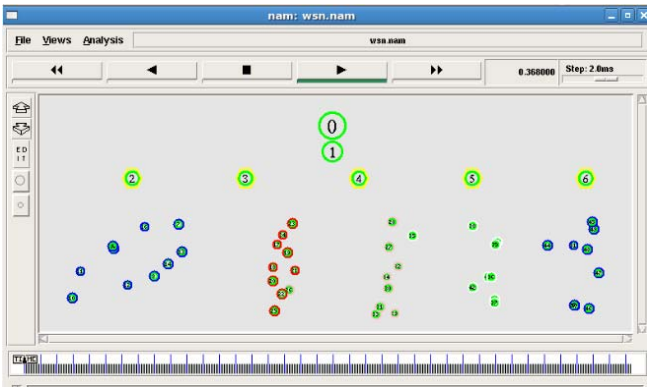

Fig 3. Hierarchal clustering of fixed nodes

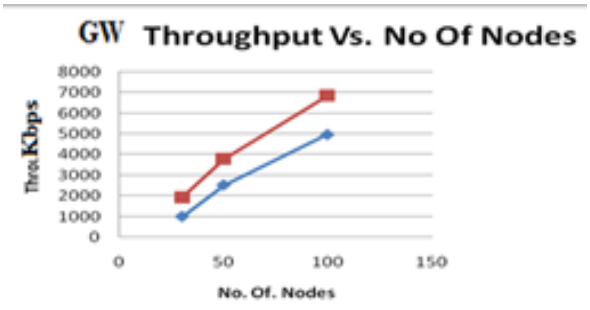

Fig 4. Throughput at Gate Way

Throughput is calculated using (total bytes *8)/(final time -start time). At gate way and cluster head throughput is increased.

V. CONCLUSIONS

In this project we are using the Hierarchical Frame work and one hop Technique, Hierarchical Frame work and one hop technique. Attack detection algorithm implemented. After simulation, performance will be compared for network throughput, packet delivery ratio, packet loss ratio and average energy consumed by the network. In this random topology, we varied Reporting Rates and performance is evaluated for different parameters. So, for random topology with 30 nodes, values of PDR, Delay, total number of packets received by the network i.e. network throughput are calculated. Better performance of PDR.

REFERENCES

[1] S. M. Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and Haekyu Rhy, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks", IEEE 2010.

[2] M Chien-Chung Su, Ko-Ming Chang, Yau-Hwang Kuo, Mong-Fong Horng,"The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks" IEEE 2005.

[3] Ilker Onat, Ali Miri, "Intrusion Detection System for Wireless Sensor Network", IEEE 2005.

[4] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks", *2003*

[5] Bo Sun and Lawarance Osborne, "Intrusion Detection Techniques in Mobile Ad Hoc Wireless Sensor Networks" , IEEE 2007

[6] Nan Kang, Elhadi M. Shakshuki, Tarek R. Sheltami "Detecting Misbehaving Nodes in MANETs" , 2010.

[7] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," *2005*