Optimizing Routing Security: A Survey

Panam R. Fadia[1], Krunal J. Panchal[2]
[1]Master Engineering in Information Technology, Gujarat Technological University, Gujarat, India
[2]Asst.Professor, PG Department, LJIET, Gujarat, India

***Abstract*- Popularity of wireless sensor networks (WSNs) is increasing continuously in different fields, as they provide efficient method of collecting valuable data from the surroundings for use in different applications. Routing in WSNs is the vital functionality that allows the flow of information generated by sensor nodes to the base station, while considering the severe energy constraint and the limitations of computational and storage resources. Indeed, this functionality may be vulnerable and must be in itself secured, since conventional routing protocols in WSNs provide efficient routing techniques with low power consumption, but they do not take into account the possible attacks. As sensor nodes may be easily captured and compromised, the classical cryptographic solutions become insufficient to provide optimal routing security, especially, for cluster-based WSNs, where cluster heads can be still among the compromised nodes. In this survey paper, we have studied few different Intrusion detection systems which provide secure routing in IDS.**

***Keywords*- Wireless sensor network, Hierarchical WSN, cluster based routing protocol, security, Intrusion detection system**

1. INTRODUCTION

Wireless Sensor Network (WSN) consists of a collection of nodes that are able to sensing, computation and wireless communication. They offer an excellent opportunity to monitor/sense the physical or environmental conditions such as temperature, sound, pressure etc. Autonomous sensors are distributed spatially and the pass their data through the intermediate nodes to a main location-base station. As WSN Provide a bridge between the real physical and virtual worlds, so used in applications such as battlefield surveillance in military, industrial process monitoring and control, food processing, machine health monitoring and many more[1].

WSN is build of nodes from a few to several thousand or hundreds, where each node is connected to at least one sensor. Constraints like size and cost on sensor nodes results in constrains on energy, memory, computational speed and bandwidth. Each node in WSN has a radio transceiver with an intended antenna or collection to an external antenna, battery and a microcontroller-an electronic circuit for computation. Constraints like size and cost on sensor nodes results in constrains on energy, memory, computational speed and bandwidth [12].

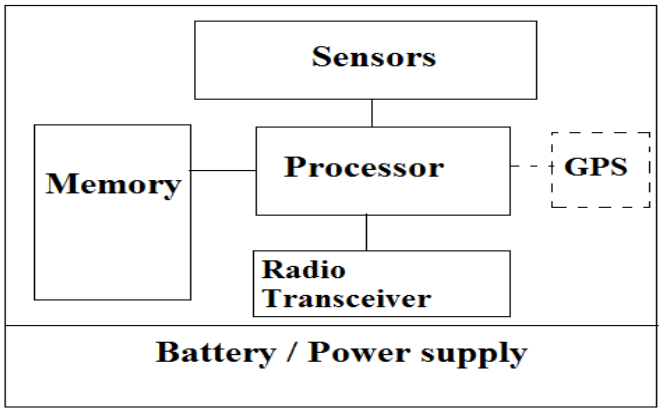

Figure 1 Basic components of WSN node

Usually sensors are small in size and inexpensive. These small sensors are not as reliable as more expensive macro sensors, but due to small size and less cost, it is capable of production and deployment in large numbers.

The nodes in WSNs are battery operated sensing devices with limited power supply and replacing or refilling the batteries is usually not an option. So, energy efficiency is one of the most important issues and designing power efficient protocols is critical for prolonging the lifetime. Normally, sensor nodes are scattered in the sensing field, in the area where we want to monitor some environmental conditions. Sensor nodes have to coordinate among themselves to get information about the physical environment. The data collected by sensor nodes is routed to the Base Station either directly or through other sensor nodes. The Base Station is either a fixed node or mobile node, which connects the sensor network to an infrastructure networks or to the Internet where users can access data and process it achieve some result as shown in Figure 2.

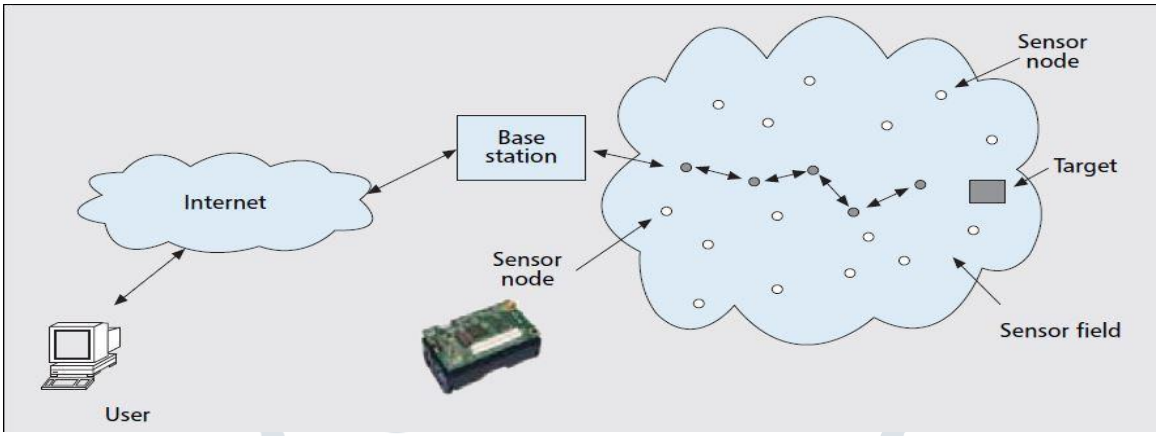

Figure 2 An example of sample WSN [2]

2. CHALLENGES IN ROUTING AND DESIGN ISSUES OF WIRELESS SENSOR NETWORK [8]

Though having wide ranges of applications, these WSN networks have several restrictions such as limited computing power, limited energy, and limited bandwidth of wireless links connecting sensor nodes to each other. One of the main design goal of WSN is to carry out data communication with the effort of prolonging the lifetime of the network. The design of routing protocols is effected by many parameters.

Energy consumption: sensor nodes can only use their limited supply of energy performing computations and transmitting information in a wireless environment. Here, this needs energy conserving communications and computation. Sensor node lifetime shows a strong dependence on the battery life time. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Node deployment: Node deployment in WSNs is totally application dependent. The deployment can be either randomized or deterministic. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. While, in random node deployment, sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

Scalability: There would be order of hundreds or thousands of sensor nodes deployed in wireless network. Any routing scheme must be able to work with this huge number of sensor nodes. The main concern is that sensor network routing protocols should be scalable enough to respond to events in the environment.

Data Reporting Model: Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting can be classified as either time-driven (continuous), query-driven, event-driven, and hybrid. The routing protocol is highly influence by the data reporting model with regard to energy consumption and route stability. The routing protocol is highly influenced by the data reporting method in terms of route calculations and energy consumption.

Fault Tolerance: Some sensor nodes may fail or be blocked due to conditions like insufficient battery power, physical damage, or environmental interference. Due to failure of sensor nodes, overall task of the sensor network should not affect. If multiple nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection BSs. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or re-routing packets through part of the network where some more energy is available

Quality of Service: In some applications, data should be delivered within a certain time limit from the moment it is sensed; otherwise the data will be pointless. Therefore bounded latency for data delivery is another important condition for time-constrained applications. However, many applications consider saving of energy, which is directly related to network lifetime, is relatively more important than

the quality of data sent. As the energy getting used, the network might be required to reduce the quality of the results to reduce the energy dissipation.

Data Aggregation: Since sensor nodes may generate significant redundant data, to reduce the number of transmissions similar packets from multiple nodes can be aggregated. Data aggregation is the combination of data from different nodes according to a certain aggregation function. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols.

3. ROUTING IN WSN [9]

The main task of sensor node is to sense data and sends it to the base station in multi hope environment for this routing is very essential. For computing routing path from sensor node to Base station (BS), there are number of routing protocols exist. Routing protocols are categorized mainly into 1) Based on Network structure and 2) based on Protocol Operation.

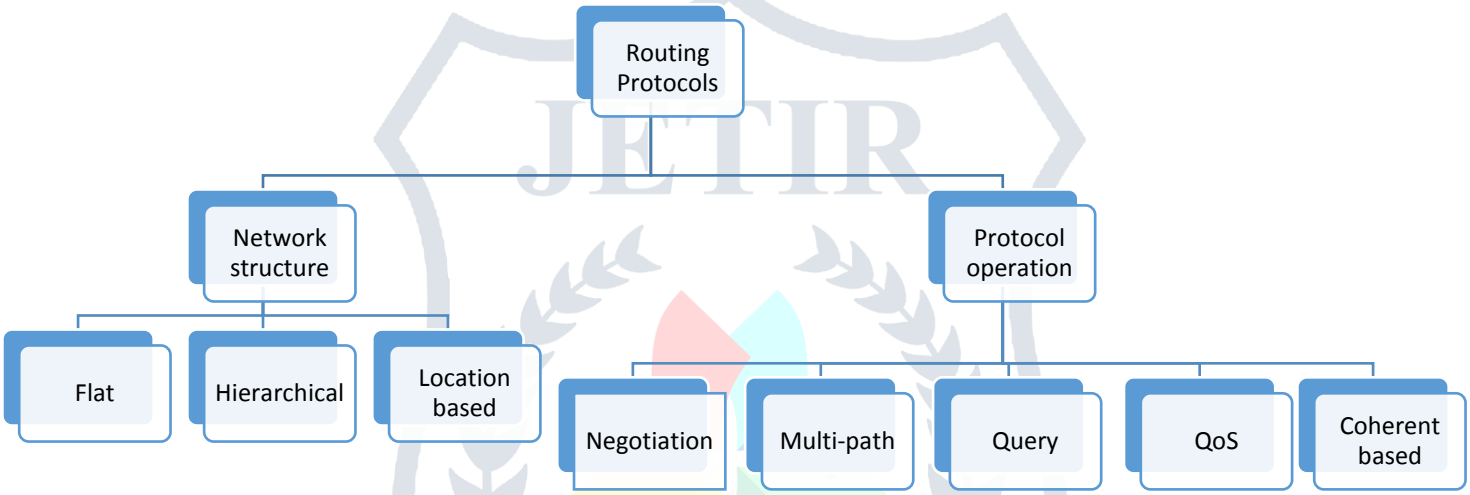

Figure 3 Routing protocols classification of in WSN [9]

All the routing protocols are very useful for computing routing path, which highly affect the WSNs performance. So, development of the routing protocol should be concentrating on balancing the load among all the sensor nodes and prolonging the network lifetime.

Here, we are focusing on Hierarchical routing protocols.

3.1 Hierarchical Routing Protocols

Hierarchical routing protocols are the most energy efficient among rest of the protocols for WSN. In, hierarchical routing protocol, network is divided into no. of clusters and every cluster has its own cluster head. This Cluster Heads (CH) are higher energy nodes, which aggregate, process and transmit the information to the BS, while lower energy nodes used to sense the targeted area and send the gathered data to the CH. Opting hierarchical routing is an efficient way to reduce the total energy consumption of the network. Here, data aggregation and processing done by CH greatly reduced the total number of messages sent to BS. The actual goal of developing hierarchical routing protocol is to minimize the network traffic to the BS.

Low energy adaptive clustering hierarchy (LEACH)

Low energy adaptive clustering hierarchy (LEACH) [4] is one of the very first hierarchical routing protocol. LEACH includes distributed clustering and also utilizes randomize rotation of cluster heads to evenly distribute the energy load within the network. It calculates a threshold value to elect the cluster head. LEACH operates in a sequence of rounds. . In each round, we find two phases 1) set-up phase and 2) steady-state phase.

In set-up phase, clusters are dynamically elaborated. It is decided for each node that they are capable for being CH in the present round or not. This decision based on whether this node has recently acted as CH, and on if it has a sufficient residual energy. Each candidate of CH sends an advertising message (ADV) to the nodes of its neighborhood, informing them about its current state. Every member node chooses its cluster head, basing on the signal strength of the corresponding ADV message that should be the greatest. This positive response is displayed by sending a joining message (JOIN) to the elected CH. On receiving all JOIN messages, each CH generates a TDMA (Time Division Multiple Access) scheduling frame and sends it to its member nodes. This allows the indication of the right data transmission time for each of them.

In steady-state phase, in each cluster, if the member node allocates a TDMA slot, it sends its data to the CH. Otherwise; it keeps its radio device turned off to save energy. Next, all CHs apply aggregation and compression functions on all data messages they received, and finally, they send the resulting messages directly to the base station. By using the concept of the random rotation of the CH roles, LEACH prevents that nodes acted as CHs die rapidly, and ensures a uniform dissipation of nodes energetic reserves. This protocol is very useful for the applications, where constant monitoring is needed. But LEACH did not fully consider the state of neighbors in the cluster-heads decision.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS protocol [5] is a variant of LEACH protocol. It adopts a particular hierarchical topology in which, nodes are organized into chain structure. In this structure nodes have adopted greedy strategy, so that each sensor node sends its data to the closest neighbor node in the next level making a chain towards the BS. Data are gradually aggregated as they transit on the established chain. This routing protocol has the advantage that it saves the spent energy in periodic clusters formation in LEACH. Nevertheless, it suffers from certain anomalies, in terms of the significant delay for the far situated nodes from the BS, and the ignorance of the energy status of the next hop node.

Optimized Energy Efficient Routing Protocol (OEERP)

Optimized Energy Efficient Routing Protocol (OEERP) [6] is also a hierarchal routing protocol which reduces the number of broadcasting messages to the access point and thus efficiently utilizes the energy of each sensor node. But the main distinguishing feature of this protocol is in selection of the cluster head (CH). Depending on the application, sensing and transmitting intervals can be modified to optimize the energy usage thereby prolonging the overall lifetime of the network. The protocol can be said to have three phases, Cluster Formation Phase, Information Processing Phase and Data Dissemination Phase.

In cluster Formation Phase of OEERP, some of the sensor nodes are randomly selected as a cluster-heads and these cluster-heads broadcast the ADV_CH packet to all the sensor nodes. Based on signal strength / or the shortest distance between the sensor node and the cluster-head, the sensor nodes join under the nearest cluster-head group by sending the JOIN_REQ packet to cluster-head to form a cluster.

These randomly selected cluster-heads process the information up to certain time period until new cluster heads are selected. This time period /time-slot can be chosen depending on the overall expected lifetime of the WSN. This process of changing the cluster head is repeated for every time-slot thereby every node gets an opportunity of becoming cluster head. This kind of approach could lead to uniform drain of node energies.

In Information Processing Phase, each and every sensor node involves in sensing the attribute and sending this information to the cluster-head of the respective cluster. Then the cluster-head performs the aggregation

In Data Dissemination Phase the aggregated information from each cluster-head is passed to the access point based on dissemination interval chosen.

Table 1 Comparison between hierarchical routing protocols

Routing Protocol	Power Usage	Plus points	Minus Points
LEACH [4]	Maximum	• self organizing adaptive clustering algorithm • good network lifetime • successfully distributes energy-usage among the nodes	• not applicable to network deployed in large regions • it assumes that all node begin with same amount of energy • no uniform distribution of cluster head • cluster head selection is random so it is possible that node with less energy may be chosen and that makes node die earlier
PEGASIS [5]	Maximum	• optimal chain based protocol • eliminates dynamic cluster formation overhead • only one transmission to the BS per round • better network lifetime than LEACH • Performs better as the size of network increases	• introduces inordinate delays to the data of nodes that are located far away from the chain leader • suffers from the problem of single point becoming bottleneck • When a head node is selected its energy level is not considered • Not energy efficient
OEERP [6]	Limited	• efficiently utilizes the energy of each sensor node by reducing the number of broadcasting messages to the access point • lead to uniform energy consumption of all the CHs over different time slot • sensing and transmitting intervals can be modified to optimize the energy usage thereby improving the overall network lifetime	• not applicable to effective multi path data delivery to the access point • there would be chances of energy gap situation in cluster formation due to which transmitting data would consume large amount of energy

4. ROUTING SECURITY IN WSN

Main security threats in WSN are: 1) Radio links are insecure and eavesdropping / injecting faulty information is possible in network. 2) Sensor nodes are not temper resistant .If it is compromised the attacker obtains all security information. Protecting confidentiality, integrity, and availability of the communications and computations is their motto keeping in mind that energy is very limited resource.

4.1 Routing attacks [1]

Due to lack of human monitoring of the network, it is possible to easily compromised sensor network. The attacks can be classified as active, passive, external and internal.

Active: The attacker exploits the weak link in the security protocol to launch attacks like packet modification, replaying etc.

Passive: The attacker obtains access to information without being detected. It is a kind of attack which is difficult to detect.
External: The attacker is external entity and has no rights to access the network.
Internal: The attacker gets authorization to access the network and deploys malicious node to compromise the sensor nodes and takes control of the network.

Name	**Characteristics**
DoS attack	Flooding, misdirection and jamming
Black hole/Sinkhole	Create illusion of Shortest path, drop the packets
Selective forwarding	Drops the packet selectively
Wormhole	Offer less number of hopes and less delay which is fake
Sybil	A malicious node pretends to be more than one node
The node replication	Make total replica of a node with the same cryptographic secrets
HELLO flood	Flood with HELLO packets

Table 2 various known Security attacks [1], [9]

4.1.1 Denial of Service (DoS) Attacks

In this attack, attacker behaves in such a way to provoke exhaustion of node's resources like causing exhaustion of battery or the overflow of routing table. Other DoS attack are jamming and tampering attacks. Jamming is the deliberated disturbance in the wireless communication channel. Sensor nodes are very vulnerable against this type of physical attack. Tampering is another type of physical attack, which targets the actual hardware of the sensor nodes. It is difficult to detect whether any particular DoS situation is caused intentionally or unintentionally, which remains an open issue.

4.1.2 Black hole/sinkhole attack

In this attack, a malicious node acts as a black hole to pull in all the traffic in the network. The attacker listens to all the route requests which are in range and then replies to the target node informing that it has the shortest path to the base station. A victim node is trapped to select it for routing its packets. Once a malicious node puts itself between the base station and sensor node, it is able to do whatever it wants like-drop all the received packets, change the content of packet etc. with the packets that pass through it. This kind of attack can be very harmful for sensor nodes that are deployed considerably far from the base station.

4.1.3 Selective forwarding attack

Selective forwarding occurs when a compromised node drops a packet that is bound for a particular destination. In this way, an attacker filters traffic from a particular area of the network. There is possibility of dropping all the packets or randomly dropping packets. Though random dropping is less dangerous, it is harder to reliably detect and trace.

4.1.4 Wormhole attack

In this type of attack, a malicious node tunnels messages between two different parts of the network with the help of a high speed link. This can make distant nodes seems to be closer in the network, which can be very helpful in a Sybil attack. If the attacker is positioned cleverly, it can damage the entire network by diverting traffic from the BS.

4.1.5 Sybil attack

Here, a malicious node pretends to be a number of different nodes in the network. The malicious node can have identities either by fabricating new ones or taking others identity as well. For attacking any node, the malicious node would use the fake identity to communicate directly with legitimate nodes, or the malicious node advertises that it has a path to the impersonated node with the help of indirect communication.

4.1.6 The node replication attack

In this particular attack, an attacker tries to add one or more nodes in a network that use the same cryptographic secrets as any other legitimate node in that network. This kind of attack may have created severe damage, like corruption of data by the adversary or even disconnection of some critical parts of the network. As sensor nodes are constrained in terms of resources and usually deployed in unattended/public environments, they can easily be captured, analyzed and extracted their secrets.

4.1.7 HELLO flood attack

In this particular attack, an attacker with a large radio range and enough processing power can send HELLO packets to a large number of sensor nodes by flooding an entire section of the network. It gives them impression that it is their direct neighbor.

4.2 Why routing security of WSN differs from other networks? [13]

- Routing in WSNs is more challenging due to the specific characteristics that distinguish WSNs from other wireless networks like cellular networks or ad hoc networks. Many new protocols have been proposed, taking into limitations and requirements of WSNs along with the application and architecture. Following are some important differences between them
- In ad hoc networks, every node is usually managed and handled by a human user. However, in a sensor network, every node is working totally independent by sending data and receiving control packets from a central system Base station (BS), which is managed by a human user.
- Batteries and computing resources are more constrained in sensor nodes than in ad hoc nodes.
- The purpose of sensor networks is very specific: measure the physical information (such as temperature, sound, ...) of its surroundings. Resulting, both hardware modules and communication/configuration protocols to be highly specialized.
- Node density in sensor networks is higher than in ad hoc networks. But, sensor nodes have more chances to fail and disappear from the network, due to the battery constraints and the low physical security.

4.3 Intrusion Detection in WSN

Intrusion detection is the process of discovering, analyzing, and reporting unauthorized or damaging network or computer activities. Intrusion detection discovers violations of confidentiality, integrity, and availability of information and resources. Intrusion detection demands:

- Constant improvement of technologies and processes to match pace of Internet innovation
- As much information as the computing resources can possibly collect and store
- Experienced personnel who can interpret network traffic and computer processes

There are three main techniques that IDS can use to classify the attacks [1].

1) **Misuse detection**: In this type of detection the action/behavior of nodes is compared with known attack patterns. In this case, attack patterns must be defined and given to the system. The disadvantages are 1) that this technique needs the knowledge of to build attack patterns and 2) they are not able to detect novel unknown attacks, and signatures database should be updated regularly.

2) **Anomaly detection:** In this technique of detection comparison of behavior of observed nodes with normal behaviors or we can say profile of the node rather than attack patterns is done. Here, it first describes normal behaviors which are obtained by automated training and then flags as intrusions any activities varying from these behaviors. The disadvantages of this technique are that system can exhibit legitimate but unseen behavior which leads to false alarm cases. Also an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives.

3) **Specification-based detection:** In this technique it combines the aims of misuse and anomaly detection. It is based on deviations from normal behaviors which are defined by neither machine-learning techniques nor training data. The specifications of attacks are defined manually that describe what normal behavior is and monitor any action according to these specifications. The drawback of this model is manually development of attack specifications is too time-consuming process for human beings.

4.4 Summary of some Intrusion Detection Systems

In order to respond to the need to intrusion prevention in WSNs, many researchers have proposed several solutions.

In [10], energy efficient hybrid IDS (eHIDS) is introduced. This detection scheme combines both misuse and anomaly detection rules in order to identify abnormal data transfer in hierarchical WSNs. eHIDS agents are implanted only on clusters heads, which reduces

energy consumption significantly. The anomaly detection model includes general attacks on integrity, delay and transmission range. Whenever an intrusion is detected, decision making module will generate an alarm. Authors claim that the proposed IDS has high detection rate, while it hasn't been evaluated with specific and various attacks.

In [11], a light weight ranger intrusion detection system is generated to link between ontology concept and intrusion detection system. . It is characterized by a particular architecture; the network should have one primary cluster head (PCH), ranger nodes(RN), member nodes(MN). This RIDS(Ranger Intrusion Detection System) mainly focuses on to detect Sybil attacks. Here, PCH is responsible for connectivity between WSN and base station communications. They also control ranger nodes. Ranger nodes collect information regarding respective member sensor nodes either periodically or non-periodically as per requirement. These ranger nodes sends isolation table to PCH time to time. Member nodes, who responsible for sensing the whole environment also translates information to ranger nodes after integration,. If any exception of PCH is occurred, MN will raise alarm the amounts of MNs reaching threshold value.

In [3], a novel anomaly detection based security scheme for large scale sensor networks that exploits their stability in their neighborhood information. If each node can built a profile of its neighbor's behavior, these profiles would help to detect changes in them by monitoring received packet power levels and arrival rates. Here, the complexity of a detection algorithm depends on the number and characteristics of system features.

In [7], a hierarchical energy efficient intrusion detection system for detecting black hole attack is proposed. In this paper the proposed approach is based on control packets exchange between sensor node and base station. Each control packet contains the node identifier id, number of packets Nb sent to cluster head. Base station will compare this Nb of each node with the amount of packets received from its CH. In case of attack, BS will broadcast an alarm to all network nodes. The alarm packet contains id of detected CH. This proposed system is energy efficient as well as helps in detecting selective forwarding attack.

In [13], a novel technique to optimally watch over the communications of the neighbor sensor nodes is proposed on certain scenario. They have proposed a new technique called spontaneous watchdog, where some nodes are able to choose independently to monitor the communications in their neighborhood. For the sake of performance detection entities called agents are divided in to two types global and local. Local agents are responsible to monitor local activities and the information sent and received by the sensor. Global agents should watch over communications and behaves as a watchdog. This technique relies on the broadcast nature of sensor communication. Here anomaly detection technique can be used for monitoring certain parameters and limits.

Table 2 Comparison of IDS we studied

S. No	Title	Author	Technique of IDS	Plus point	Minus point
1	Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks	Abror Abduvaliyev, Sungyoung Lee and Young-Koo Lee	Hybrid	Significantly reduces the total amount of energy consumed in all nodes in the network	Not implemented in real network and in radio jamming condition
2	A Light-weight Ranger Intrusion Detection System on Wireless Sensor Networks	Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen	Anomaly based	Effect of ontology can be observed in Sybil attack detection at whole relationship levels of wireless sensor network	Much more needs to be known about constructing ontology to detect different attacks
3	Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs	Samir Athmani, Djallel Eddine Boubiche, Azeddine Bilami	Specification based	Can mitigate significantly black hole attack, selective forwarding attack and secure the routing process	Reduce the impact of black hole attack to only 2 percent
4	Applying Intrusion Detection Systems to Wireless Sensor Networks	Rodrigo Roman, Jianying Zhou and Javier Lopez	Signature based	Not all packets can be overhead by a global agent, due to randomness of the selection process	Doesn't assure that one and only one node will activate its global agent foe every packet in network
5	An Intrusion Detection System for Wireless Sensor Networks	Onat and A. Miri	Anomaly based	When the degree of anomaly increases, it's detected with higher probability and in a shorter period of time	Increases false alarm rate

4.5 Conclusion

The existing secure routing protocol in WSNs focused on presenting security system with key management schemes and cryptographic solutions. These protocols are very efficient to defense the external attacks but somehow they don't treat the insider attacks as a serious issue. It is a major drawback for these protocols that they are not capable to detect compromised node in the network.

Since an insider attacker disposes, it can have hold of the relevant cryptographic keys and any possible security material to be part of the routing path. Thus, a compromised node may success to be a CH and it can perform several attacks on an entire group of sensor nodes. Moreover, cryptographic and key management solutions which able resist the outsider attackers and reduce the impact of the insiders couldn't provide the desired security for routing in hierarchical WSNs, even if the network is having only a few malicious nodes. Thus various IDS are introduced to detect insider attacks which provide second line of defense.

Future work will involve development, implementation and simulation of a light weight intrusion detection system and deploying it on secure routing protocol.

REFERENCES

[1] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai- Choong Wong, On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013

[2] Bo Sun And Lawrence Osborne,Yang Xiao And Sghaier Guizani, Intrusion Detection Techniques In Mobile Ad Hoc And Wireless Sensor Networks, IEEE Wireless Communications October 2007

[3] Onat and A. Miri, An Intrusion Detection System for Wireless Sensor Networks, Wireless and Mobile Computing, Networking And Communications, vol. 3, 2005, pp. 253-259.

[4] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks, " IEEE Transactions on the wireless communications, Vol. 1, No 4, pp. 660-670, 2002

[5] S. Lindsey, and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", EEFAC p a p #242, Updated Sept 29,2001

[6] K. Kishan Chand, P Vijaya Bharati and B. Seetha Ramanjaneyulu, Optimized Energy Efficient Routing Protocol for Life-Time Improvement in Wireless Sensor Networks, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[7] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs, Computer and Information Technology (WCCIT), 2013 World Congress on Date 22-24 June 2013

[8] Jamal N. Al-karaki and Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Wireless Communications • December 2004

[9] Suraj Sharma and Sanjay Kumar Jena, A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks, *ICCCS'11* February 12-14, 2011, Rourkela, Odisha, India

[10] Abror Abduvaliyev, Sungyoung Lee and Young-Koo Lee, Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks, 2010 International Conference on Electronics and Information Engineering (ICEIE 2010)

[11] Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen, A Light-weight Ranger Intrusion Detection System on Wireless Sensor Networks, 2011 Fifth International Conference on Genetic and Evolutionary Computing

[12] Ismail Butun, Salvatore D. Morgera and Ravi Sankar, A servey of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Communications and Surveys & Tutorials, vol. 16, no. 1, First quarter 2014

[13] Rodrigo Roman, Jianying Zhou and Javier Lopez, Applying Intrusion Detection Systems to Wireless Sensor Networks, in Consumer Communications and Networking Conference, 2006, pp. 640-644.