SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY

[1]PRABHUDUTTA MOHANTY, [2]SANGRAM PANIGRAHI, [3]NITYANANDA SARMA and [4]SIDDHARTHA SANKAR SATAPATHY
Department of Computer Science and Engineering
Tezpur University, Tezpur, India
[1]prabhudutta.mohanty@gmail.com, [2]sangrampanigrahi.sp@gmail.com, [3]nitya@tezu.ernet.in and [4]sankar@tezu.ernet.in

ABSTRACT

Wireless sensor networks are usually deployed for gathering data from unattended or hostile environment. Several application specific sensor network data gathering protocols have been proposed in research literatures. However, most of the proposed algorithms have given little attention to the related security issues. In this paper we have explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.

Keywords: *Wireless Sensor Networks, Routing, Data Gathering, security, attack, threat model.*

1. INTRODUCTION

Application specific wireless sensor network consists of hundreds to thousands of low-power multi-functioning sensor nodes, operating in an unattended or hostile environment, with limited computational and sensing capabilities. Realization of sensor network applications requires wireless ad hoc networking techniques. However protocols and algorithms proposed for traditional ad hoc networks are not well suited due to the unique features and application requirements of sensor networks. Because of its unique features, sensor networks are used in wide range of applications in areas like health, military, home and commercial industries in our day to day life [1] [2] [3].

Data gathering protocols are formulated for configuring the network and collecting information from the desired environment. In each round of the data gathering protocol, data from the nodes need to be collected and transmitted to (BS), where from the end user can access the data. Sensor nodes use different data aggregation techniques to achieve energy efficiency. Existing data gathering protocol can be classified into four different categories based on the network structure and protocol operation: flat (Flooding [18], Gossiping [18], Directed Diffusion [20], Rumor Routing [22], SPIN [19], Energy Aware Routing [30], etc), hierarchical (LEACH [23], PEGASIS[24], TEEN[25], QCCA[26], TREPSI[27], TCDGP[28], APTEEN[31], SOP[32], TTDD[33], etc), location (GAF[29], MECN [34], SMECN[35], GEAR[36], SPAN[37], etc) based routing protocols and network flow or quality of service (QoS) aware routing (SAR[40], CEDAR[41], SPEED[42] etc).

As WSN is mostly used for gathering application specific information from the surrounding environment, it is highly essential to protect the sensitive data from unauthorized access. WSNs are vulnerable to security attacks due to the broadcast nature of radio transmission. Sensor nodes may also be physically captured or destroyed by the enemies. The uses of sensor network in various applications emphasis on secure routing. Various protocols are proposed for routing and data gathering but none of them are designed with security as a goal. The resource-limitation of sensor networks poses great challenges for security. As sensor nodes are with very limited computing power, it is difficult to provide security in WSN using public-key cryptography. Therefore most of the proposed security solutions for WSN are based on symmetric key cryptography. In this paper we have reviewed possible attacks on WSN in general as well as attacks on specific WSN data gathering protocols.

Rest of the paper is organized as follows. Section 2 gives general overview of different security issues. Section 3 elaborates possible attacks against WSN in general. In section 4 explores existing WSN data gathering protocols and security threats on them and finally section 5 concludes the paper.

2. OVERVIEW OF SECURITY ISSUES

2.1. Attack and attacker

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk.

2.2. Security requirements

A sensor network is a special type of Ad hoc network. So it shares some common property as computer network. The security requirements [3][11][15][17] of a wireless sensor network can be classified as follows:

- Authentication: As WSN communicates sensitive data which helps in many important decisions making. The receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network.
- Integrity: Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.
- Data Confidentiality: Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.
- Data Freshness: Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.
- Availability: Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.
- Self-Organization: A wireless sensor network believes that every sensor node is independent and flexible enough to be self-organizing and self-healing according to different hassle environments. Due to random deployment of nodes no fixed infrastructure is available for WSN network management. Distributed sensor networks must self-organize to support multihop routing. They must also self-organize to conduct key management and building trust relation among sensors.
- Time Synchronization: Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off periodically.
- Secure Localization: The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate non-secured location information by reporting false signal strengths and replaying signals, etc.

2.3. Security classes

Attacks on the computer system or network can be broadly classified [12] as interruption, interception, modification and fabrication (Figure 1).

- Interruption is an attack on the availability of the network, for example

physical capturing of the nodes, message corruption, insertion of malicious code etc.

- Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.
- Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with bogus data.
- Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

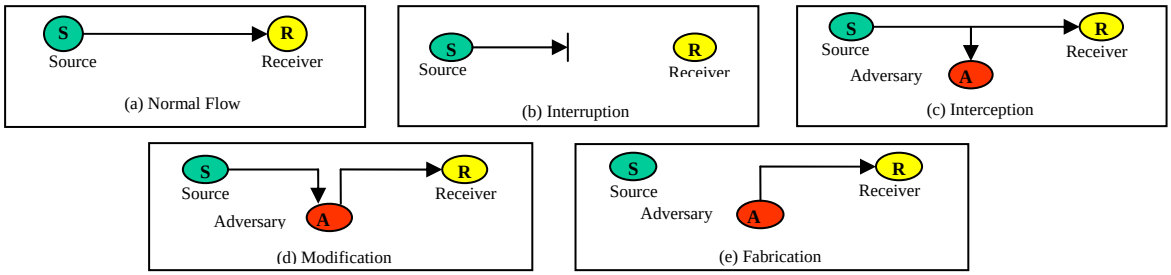

Figure 1 Security Classes

2.4. Threat models

Threats in sensor networks [13] can be classified as sensor-class (mote-class) attackers and laptop-class attacker. Another classification can be made as external threats and internal threats. Mote class attackers may be sensors with similar capabilities as sensor network. These types of attackers can jam the radio link in its immediate vicinity. An attacker with laptop-class devices have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and hence they can affect much more than an attacker with only ordinary sensor nodes. A single laptop-class attacker might be able to eavesdrop on an entire network.

External threats may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise Denial of Service (DoS) attack. Whereas inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile. Insider attacks may be mounted by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes and who then use one or more laptop-class devices to attack the network.

2.5. Layering-based attacks and possible security approach

Though there are no such standard layered architecture of the communication protocol for wireless sensor network, here we have summarized possible attacks and their security solution approaches in different layers with respect to ISO OSI layer in the table-1 [14][17].

Table 1. Layering-based attacks and possible security approach

Layer	Attacks	Security Approach
Physical Layer	Jamming and tampering	Use spread-spectrum techniques and MAC layer admission control mechanisms
Data Link layer	jamming and collision	Use error correcting codes and spread-spectrum techniques
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	injects false messages and energy drain attacks	Authentication
Application Layer	Attacks on reliability	Cryptographic approach

3. POSSIBLE ATTACKS AGAINST WSN

Most of the routing protocols proposed for ad hoc and sensor network are not designed to handle security related issues. Therefore there is a lot of scope for attacks on them. Different possible attacks [4][5][6][7][8][9][10][15][16][38][39] on the flow of data and control information can be categorized as follows:

- Spoofed, altered, or replayed routing information
- Selective forwarding attack
- Sinkhole attack
- Sybil attack
- Wormholes attack
- HELLO flood attack
- Acknowledgement spoofing
- Sniffing attack
- Data integrity attack
- Energy drain attack
- Black hole attack
- Node replication attack

3.1. Spoofed, altered, or replayed routing information

This is the most common direct attack against a routing protocol. This attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency. The standard solution for this attack is authentication. i.e., routers will only accept routing information from valid routers.

Figures 2(i & ii) show how an adversary can attract and repeal the network traffic respectively, by advertising a false path. Figure 2(iii) presents a scenario in which an adversary node creates a routing loop in the network.

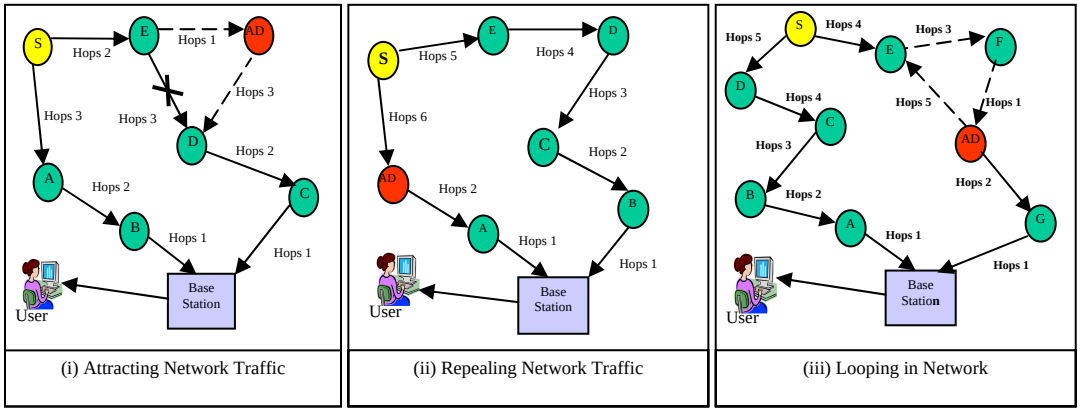

Figure 2. Spoofed Attack, Altered, Replayed Routing Information

3.2. Selective forwarding attack

Multi-hop mode of communication is commonly preferred in wireless sensor network data gathering protocols. Multi-hop networks assume that participating nodes will faithfully forward and receive messages. However a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. This attack can be detected if packet sequence numbers are checked properly and continuously in a conjunction free network. Addition of data packet sequence number in packet header can reduce this attack.

Figure 3(i) and 3(ii) show scenarios of selective forward attack. In figure 3(i), source node 'S' forwards its data packet D1, D2, D3, D4 to node 'A' and node 'A' forward these received packets to node 'B'. In other hand an adversary node AD selectively forwards packets D1, D3 while dropping packet D2 and D4. In another scenario shown in figure 3(ii), an adversary may selectively drop packets originated from one source and forward that of others.

3.3. Sinkhole attack

By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node. A compromised node which is placed at the centre of some area creates a large "sphere of influence", attracting all traffic destined for a base station from the sensor nodes. The attacker targets a place to create sinkhole where it can attract the most traffic, possibly

closer to the base station so that the malicious node could be perceived as a base station. The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighbouring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

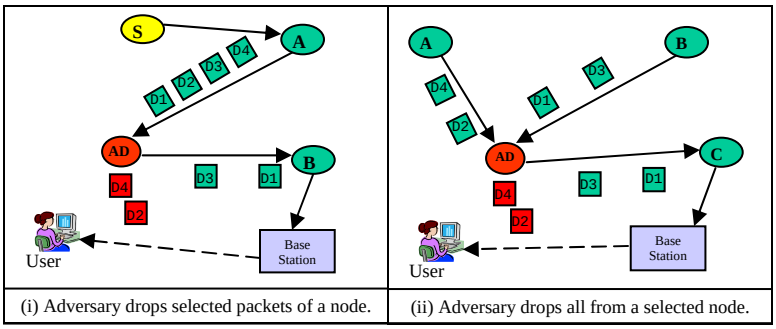

Figure 3. Selective Forward Attack

The Figure 4 demonstrates sinkhole attack where 'SH' is a sinkhole. This sinkhole attracts traffic from nearly all the nodes to rout through it.

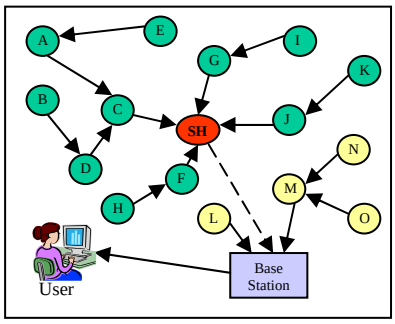

Figure 4. Sink hole Attack

3.4. Sybil attack

Most protocols assume that nodes have a single unique identity in the network. In a Sybil attack, an attacker can appear to be in multiple places at the same time. This can be convincing by creating fake identities of nodes located at the edge of communication range. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbours to construct the network. So it expects nodes to be present with a single set of coordinates, but by using the Sybil attack an adversary can ''be in more than one place at once''. Since identity fraud leads to the Sybil attack, proper authentication can defend it.

The Figure 5 demonstrates Sybil attack where an adversary node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as to 'D' so when 'A' wants to communicate with 'F' it sends the message to 'AD'.

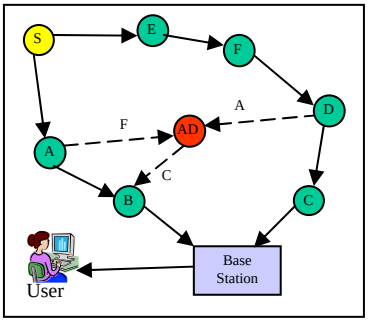

Figure 5. Sybil Attack

3.5. Wormhole attack

In this attack an adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbours, leading to quick exhaustion of their energy resources. An adversary situated close to a base

station may be able to completely disrupt routing by creating a well-placed wormhole. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor's network protocols. We can prevent this by avoid routing race conditions. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs.

Figure 6 demonstrates Wormhole attack where 'WH' is the adversary node which creates a tunnel between nodes 'E' and 'I'. These two nodes are present at most distance from each other.

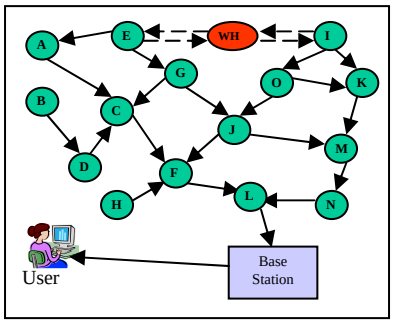

Figure 6. Wormhole Attack

3.6. HELLO flood attack

Many protocols require nodes to broadcast HELLO packets for neighbour discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbour, so that all the nodes will respond to the HELLO message and waste their energy. The result of a HELLO flood is that every node thinks the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighbouring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes. We can prevent this attack by verifying the bi-directionality of local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices. Another way by using Authenticated broadcast protocols.

The Figure 7 depicts how an adversary node 'AD' broadcast hello packets to convince nodes in the network as neighbour of 'AD'. Though some node like I,H,F are far away from 'AD' they think 'AD' as their neighbour and try to forward packets through it which results in wastage of energy and data loss.

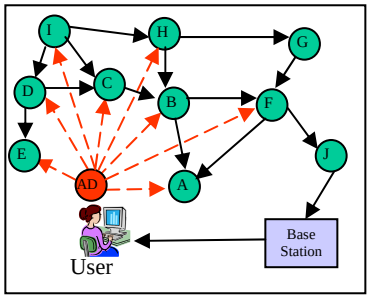

Figure 7. Hello Flood Attack

3.7. Acknowledgement spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighbouring nodes. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. This results in packets being lost when travelling along such links. The goal includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links. Acknowledgement spoofing attacks can be prevented by using good encryption techniques and proper authentication for communication.

In figure 8, node E sends data to node G. However node G is down and an adversary node AD,

knowing that node G is dead, acknowledges on behalf of G. This convene E that G is still actively receiving the packets.

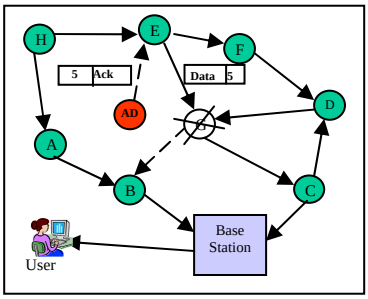

Figure 8. Acknowledgement Spoofing

3.8. Sniffing attack

Sniffing attack is a good example of interception or listen-in channel attack. In this attack an adversary node is placed in the proximity of the sensor grid to capture data. The collected data is transferred to the intruder by some means for further processing. This type of attack will not affect the normal functioning of the protocol. An outside attacker can lunch this attack for gather valuable data from the sensors. Often this attack is related to military or industrial secrets. The attack is based on the inherit vulnerability of the wireless networks of having unsecured and shared medium. Sniffing attacks can be prevented by using proper encryption techniques for communication.

Figure 9 is a pictorial representation of sniffing attack. Suppose it is an object tracking system. Node 'A' traces the object and finds a path to base station through nodes B, C and D. Node D is responsible to send the data to base station. An adversary node AD which is placed nearer to the node 'D' captures the data and sends to its data processing centre without disturbing the network.

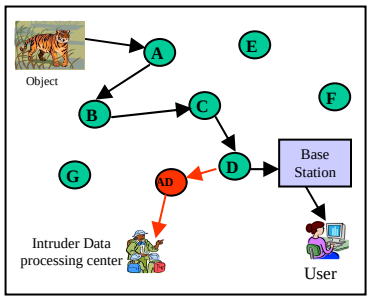

Figure 9. Sniffing Attack

3.9. Data integrity attack

Data integrity attacks compromise the data travelling among the nodes in WSN by changing the data contained within the packets or injecting false data. The attacker node must have more processing, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor data and by doing so compromise the victim's research. It also falsifies routing data in order to disrupt the sensor network's normal operation, possibly making it useless. This is considered to be a type of denial of service attack. This attack can be defended by adapting asymmetric key system that is used for encryption or we can use digital signatures, but this requires a lot of additional overhead and is difficult to adapt in WSN.

Figure 10 shows an example of Data Integrity attack. In the figure node A sends a data packet to B. This packet contains destination id (B), data (10) and packet sequence number (1). An adversary node AD modifies this data as 5 and forwards it to node B.

3.10. Energy drain attack

WSN is battery powered and dynamically organized.

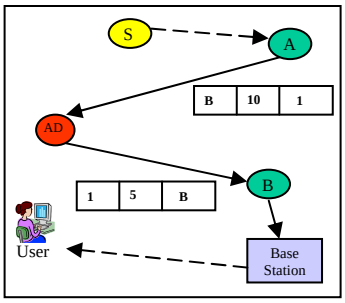

Figure 10. Data Integrity Attack

It is difficult or impossible to replace/recharge sensor node batteries. Because there is a limited amount of energy available, attackers may use compromised nodes to inject fabricated reports into the network or generate large amount of traffic in the network. Fabricated reports will cause false alarms that waste real world response efforts, and drain the finite amount of energy in a battery powered network. However the attack is possible only if the intruder's node has enough energy to transmit packets at a constant rate. The aim of this attack is to destroy the sensor nodes in

the network, degrade performance of the network and ultimately split the network grid and consequently take control of part of the sensor network by inserting a new Sink node. To minimize the damage caused by this attack fabricated reports should be dropped en-route as early as possible.

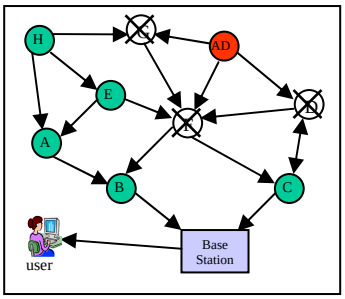

Fig 11: Energy Drain Attack

In figure 11 adversary node 'AD' generates false data continuously. Its immediate neighbour nodes 'D','F' and 'G' responds to 'AD' and finally drains there battery.

3.11. Black-hole attack

The black hole attack positions a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This attack can isolate certain nodes from the base station and creates a discontinuity in network connectivity. This attack is easier to detect than sinkhole attack. This attack generally targets the flooding based protocols. Another interesting type of attack is homing. In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbours of the base station. The attacker can then physically disable these nodes. This leads to another type of black hole attack. This attack aims to block the traffic to the sink and to provide a better ground for lunching other attacks like data integrity or sniffing. This attack can be prevented if we can restrict malicious node to join the network. Network setup phase should be carried out in a secure way.

In the Figure 12 BH is the black-hole which first convenes the network that it is the nearest node to base station and attracts the network to rout data through it. When it receives data from neighbouring nodes it drops them.

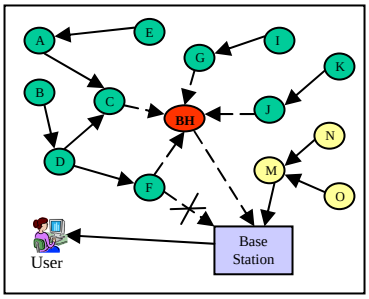

Figure 12. Black-hole Attack

3.12. Node replication attack

This is an attack where attacker tries to mount several nodes with same identity at different places of the existing network. There are two methods for mounting this attack. In first method the attacker captures one node from the network and creates clone of a captured node and mounts in different places of the network. In second method attacker may generate a false identification of a node then makes clone out of this node and mounts in different places of the network. These mounted clone nodes tries to generates false data to disrupt the network. Node replication attack is different form Sybil attack. In Sybil attack a single node exists with multiple identities but in node replication attack multiple nodes present with same identity.

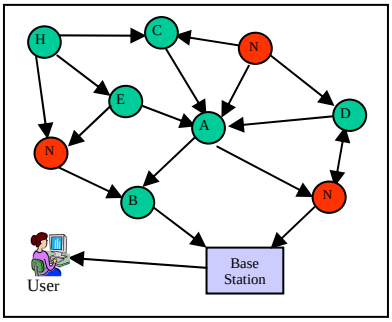

Figure 13. : Node Replication Attack

Therefore in sybil attack an attacker can succeed by mounting only a single node where as node replication attack requires more node to be mounted throughout the network this increases the chance of detection. This attack can be avoided if we centrally compute the data gathering path by the BS then multiple place occurrence of the node can be detected. The other way to detect the attack is verifying the identities (authentication) of nodes by a trustworthy node.

In the Figure 13 N is the identity of cloned nodes which are mounted in multiple places in the network to bias the entire network.

4. POSSIBLE ATTACKS ON EXISTING PROTOCOLS

Depending on the network architecture and information used while taking routing decision, routing protocol in WSNs can be classified into flat-based routing, hierarchical-based routing, location-based routing, and network flow or quality of service (QoS) aware routing. Some of the protocols follow the characteristics of more than one class, because of which classifications may not be completely distinct and they may overlap on each other. For example one of the hierarchical protocol PEGASIS, which is classified as hierarchical protocol also uses location information for forming a chain like path of the nodes. Instead of classify them under location based routing protocol, we preferred to classify them under hierarchical based routing the communication pattern they follow.

4.1. Flat based routing protocol

Flat routing assumes that nodes have uniform responsibility in the network. Sensor nodes relying on some short of flooding mechanism to spread query request in the network for gathering information. As a huge number of nodes are deployed in WSN, data is usually transmitted from every sensor node with significant redundancy. This type of protocols consumes more energy than others and therefore in order to minimize energy consumption, nodes aggregate data during transmission. Protocols that may be classified under this category are: Flooding [18], Gossiping [18], Directed Diffusion [20], SPIN [19], Rumor Routing [22], The Minimum Cost Forwarding Protocol [21], Energy Aware Routing [30] etc.

4.1.1. possible attacks on flat based routing protocols

In flat routing nodes need to exchange hello packets among themselves to discover neighbours for charring out data communication. An adversary node may join during neighbour discovery phase and convince neighbouring node to be the nearest to them, so as to forward data towards it and hence implant sinkhole attack. In the neighbour discovery phase of the flat routing protocol adversary nodes may join the network with false node identity and appear with multiple identity to its neighbour leading to Sybil attack. In flat routing all communication happens to be neighbour-to-neighbour. With the help of two adversary node attacker can create tunnel in the network, this is possible by convincing nodes as neighbours of adversary node. This helps to introduce Worm hole attack in the network. Exchange hello packet gives a better ground for mounting hello flood attack. Sniffing attack is a common attack which can mount successfully with less effort. If an adversary placed near the base station it can easily capture the data without disturbing the network. In case of the flat routing most of the protocol follows data flooding technique, this gives a better ground for the sniffing attack to be mounted. Multi-path data delivery leads to easy data integrity attack. If an adversary changes the data in one path then it puts a question mark on the reliability of the data. In this attack attacker needs to identify the path of communication and put adversary in that path to change the data. An adversary can generate false data or query by joining the network. When a node responds to these wrong data or query, leads them to suffer from the energy drain attack. Flat routing is more susceptible to this type of energy drain attack due to there pattern of communication. In flat routing protocol, an adversary node placed near the base station can attract entire network traffic to mount the black hole attack. Attacker can mount adversary nodes with same id or false id in different place of the network. These nodes generate the false data and disrupt the data communication. It puts a question mark on data integrity also. Flat routing suffers from data integrity attack as node can be mounted in arbitrary position in the network and includes them in the network in neighbour discovery phase.

4.1.2. attacks may not be applicable on flat based routing protocols

As most of flat based routing protocols follow multi-path data delivery or data flooding technique, we expect successful data delivery at the base station even if there is some faulty path. Therefore Spoofed, altered or replayed routing information attack as well as Selective forward attack are not fruitful for the flat based routing protocols. Usually to ensure reliability acknowledgement is expected for each successful data delivery. In case of flat routing most of the protocols, node floods data with in its neighbourhood. Therefore data delivery is expected without depending on the

acknowledgement and hence Acknowledgement spoofing attack may not be successful here.

4.2. Hierarchical protocols

In hierarchical-based routing, nodes in the network play different roles in different instance of time. The hierarchical routing conserves energy by adopting multi hop communication, data aggregation and fusion in WSN. In this architecture low energy nodes perform the sensing and communicating in a short range where as higher energy nodes process and send the information in long range. Hierarchical routing increases overall system scalability, lifetime, and energy efficiency of WSN. It also reduces number of transmissions. Hierarchical routing is usually a two-phase routing where one phase is used to select the cluster-heads and the other one is used for routing. Few protocols coming under this category are LEACH [23], PEGASIS [24], TEEN [25], APTEEN [31], SOP [32], TREPSI [27], TCDGP [28], QCCA [26], TTDD [33], etc.

4.2.1. possible attacks on hierarchical protocols

In case of hierarchical routing, network topology may depend on communication range of the nodes, location information, distance between the nodes and remaining battery power. An adversary can manipulate these parameters to mount spoofed, altered, or replayed routing information attack and attract the network towards it to create a sinkhole. This sink hole may turn into black hole if it absorbs the data completely. These protocols transmit data in multi-hop so intermediate nodes take the responsibility of data aggregation/fusion and forward data to upper level. An adversary who joins the network in setup phase can selectively forward data to upper level and change the data to lead data integrity attack. In hierarchical based routing nodes collaborate among themselves to form the multi-hop routing. For this node collaboration they need to know their node identities. This gives a better ground for the adversary nodes to appear with multiple identities in the network and make Sybil attack trivial. Attacker can mount adversary nodes with same id in different place of the network and actively join the network. These nodes generate the false data and disrupt the data communication. The protocol where data communication path is computed centrally by the base station (TREEPSI) can easily detect/avoid this attack. Nodes try to collaborate with its nearest neighbour which can forward the data to the base station. An adversary can convince nodes as closest neighbour and force them to forward data through it. Finally this adversary may replay this data at another part of the network by creating tunnel with the help of the adversary nodes. This makes wormhole attack trivial in hierarchical routing. Neighbour discovery is a vital part of hierarchical routing protocol. For neighbour discovery hello packets need to be exchanged between the nodes. A laptop class adversary can take the benefit of this and flood hello packets in the network to convince the nodes as its neighbour. With the help of this adversary energy drain attack can be mounted. Even if hierarchical routing follows multi-hop, it depends node to node communication as well. Therefore whenever a node sends data to another node, it expects an acknowledgement from the receiving node. Adversary nodes may take the benefit of this and send false acknowledgement for weak and dead nodes to convince the network as alive. Leader nodes take the responsibility of forwarding data to the base station. They transmit with sufficient power to reach the base station. So if an adversary is placed near the base station it can easily capture data and send it to intruder base station for further processing.

4.3. Location-based protocols

In location based routing, sensor nodes are addressed by their locations. Most of the routing protocols conserve energy by transmitting to the nodes within neighbouring area. The distance between neighbouring nodes can be estimated on the basis of incoming signal strengths or accurately with the help of GPS. Coordinates of neighbouring nodes can also be obtained by exchanging location information between neighbours. Here entire network is divided into small grids. In case there is no activity in a grid, nodes within that grid enter in to sleep mode to conserve energy. If the region to be sensed is known, using the location of sensors, the query can be diffused only to that particular region which will eliminate the number of transmission significantly. Location based routing protocols are well applicable to sensor networks where there is less or no mobility. Some example of the above type is MECN [34], SMECN [35], GAF [29], GEAR [36] and SPAN [37] etc.

4.3.1. possible attacks on location-based protocols:

To save energy, some location based schemes demand that nodes should go to periodic sleep if

there is no activity. An adversary node can take the benefit of this and convince nodes to go to sleep mode. This leads certain region unavailable to base station. Attacker succeeds to mount black hole and selective forwarding attack. Adversary nodes can generate false location information and join the network to mount Sybil attack. In this type of protocols nodes in a grid communicate with each other and with other grids. This requires hello packet exchange between neighbours. An adversary may take the advantage of this to mount HELLO flood attack. Grids communicate with the help of co-coordinator node. An adversary takes the advantage of this to create a wormhole and tunnels data from one part to another part of the network. If an attacker places an adversary near the required grid then it can capture the data of that particular grid. It is better to place an adversary near the base station where it can capture data from all the regions. Basically in this category of protocols query is placed to certain region based on the location information. So an adversary can generate false query and send to the targeted area of the network. The nodes present in this region responds to the query and drains their battery. Similar to the case of hierarchical routing whenever a node sends data it expects an acknowledgement. Adversary nodes may take the benefit of this and send false acknowledgement for weak and dead nodes to convince the network as alive.

4.3.2. attacks not applicable on location-based protocols

In location based routing protocol most of the protocol use GPS to find the location of the node. It is assumed that location information is accurate due to use of GPS. On the basis of this information network grids are formed to carry out communication. Therefore it is difficult for an attacker to mount spoofed, altered or replayed routing information attack, sinkhole attack and node replication attack.

4.4. Network flow and QoS-aware protocols

In QoS-based routing protocol, route setup is designed as a network flow problem. The sensor network paths are obtained by balancing energy consumption and data quality. The network has to satisfy certain QoS metrics, e.g., delay, energy, bandwidth, etc. when delivering data to the BS. To avoid single route failure in QoS-based routing protocol, multi-path approaches as well as localized path restoration schemes are used. Some of protocols categorised under this category are SAR [40], CEDAR [41], SPEED [42] etc.

4.4.1. possible attacks on network flow and QoS-aware protocols

In these protocols network paths setup is based on balance between energy consumption and data quality. Therefore adversary can generates false energy information and bandwidth to attract nodes to include her in the path and send data through it. This helps to create sink hole in the network. Attacker can ultimately convert this sink hole to black hole. Like sinkhole worm hole can be created by generating false messages. Once the sinkhole attack is mounted successfully one can make selective forward attack trivial. In order to construct routing path, nodes need to share information like energy level and data quality. Another point is that, these protocols do localized path restoration to maintain routing path for which hello packet need to be exchanged between the nodes. So adversary can take the benefit of these to mount the hello flood attack. Data transmission is multi-hop mode in network flow and QoS-aware protocols. For reliability in data communication acknowledgement is required. An attacker takes the benefit of this and can mount acknowledgement spoofing attack to bias the network. The attacker can place an adversary near the network grid to capture data and send for further processing to the intruder base station. Multi-hop data delivery leads to easy data integrity attack. Any intermediate compromised node can change the data to lead data integrity attack. Multiple adversary nodes can be mounted in different place of the network with same identity. This node replication attack can help the attacker to drain the battery of neighbour nodes by generating false data and routing information.

4.4.2. attacks not applicable on network flow and QoS-aware protocols:

Since most of these protocols follow multi-path approach and localized path restoration schemes so we expect it is difficult for the adversary to bias routing. If an adversary node tries to exist with multiple identities can be easily detected due to localized path restoration.

The summarized report of the different attack on the protocols is given below in table 2. A tick mark entry in the table indicates that a protocol coming under the class of the protocol may suffer from the corresponding attack, where as a cross

mark indicates that the protocol is immune from the attack. In our extensive study we found that hierarchical protocols suffer from all the attacks. However individual protocols classified under hierarchical group may not suffer from all the attacks. Like that location based protocols can defend more attacks than other protocols. But these protocols have drawback of using GPS. This may lead to complicacy in design as well as expensive sensor nodes.

Table 2. Class of routing protocols and possible attacks

Protocol	Possible Attacks											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Flat Based Routing	×	×	√	√	√	√	×	√	√	√	√	√
Hierarchical	√	√	√	√	√	√	√	√	√	√	√	√
Location-Based	×	√	×	√	√	√	√	√	×	√	√	×
Network flow and QoS-aware	×	√	√	×	√	√	√	√	√	√	√	√

1. Spoofed, altered, or replayed routing information, 2. Selective forward, 3. Sink hole, 4. Sybil, 5. Worm hole, 6. HELLO flood, 7. Acknowledgement spoofing, 8. Sniffing, 9. Data integrity, 10. Energy drain, 11. Black hole, 12.Node replication attack.

5. CONCLUSIONS

This paper outlined different security issues in wireless sensor network in general and made an extensive study of different threats associated with existing data gathering protocols. As these protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Even some of the protocols are seems to be vulnerable to most of the attacks. Similarly some attacks like HELLO flood, Acknowledgement spoofing and sniffing can be used by the adversaries to affect most of the protocols.

6. ACKNOWLEDGMENT

This work is funded by AICTE (F.No. 8023/BOR/RID/RPS-212/2007-08).

REFERENCES:

[1] Lin, R., Wang, Z. & Sun, Y., (2004) "Wireless Sensor Networks Solutions for Real Time Monitoring of Nuclear Power Plant in", *The Proceedings of the 5' World Congress on intelligent Control and Automation*, Hangzhou, P.R. China.

[2] Römer, K., Mattern, F. & Zurich, E., (2004) "The Design Space of Wireless Sensor Networks", *IEEE Wireless Communications*.

[3] Yoneki, E. & Bacon, J., (2005) "A survey of Wireless Sensor Network technologies: research trends and middleware's role", technical report. *http://www.cl.cam.ac.uk/TechReports*, ISSN 1476-2986.

[4] Kaplantzis, S., (2006) "Security Models for Wireless Sensor Networks", *http://members.iinet.com.au/~souvla/transfer-final-rev.pdf*

[5] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., (2000) "Protocols for Self-Organization of a Wireless Sensor Network", *IEEE Personal Communications*, pp. 16-27.

[6] Woo, A. and Culler, D., (2001) "A Transmission Control Scheme for Media Access in Sensor Networks", *Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001)*, Rome, Italy.

[7] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. & Chandrakasan, A., (2001) "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, Rome, Italy, pp. 272-287.

[8] Shen, C., Srisatjapornphat, C., and Jaikaeo, C., (2001) "Sensor Information Networking Architecture and Applications", *IEEE Pers. Communication*, pp. 52–59.

[9] Committee on National Security Systems (CNSS), (2006) *National Information Assurance Glossary*, NSTISSI,No. 4009.

http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[10] Wood, A. and Stankovic, J. A., (2002) "Denial of Service in Sensor Networks", *IEEE Computer*, 35(10):54-62, pp. 54-62.

[11] Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V., (2007) "Wireless sensor network security - a survey", *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, CRC Press.

[12] Stallings, W., (2000) *Cryptography and Network Security Principles and Practice*, Cryptography Book, 2nd Edition, Prentice-Hall, 0-13-869017-0.

[13] Karlof, C., and Wagner, D., (2003) "Secure Routing in Sensor Networks: Attacks and Countermeasures", *SNPA*, pp. 1-15.

[14] Saxena, M., (2007) "Security in Wireless Sensor Networks – A Layer based classification", Technical Report [CERIAS TR 2007-04], *Center for Education and Research in Information Assurance and Security - CERIAS*, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf

[15] Fernandes, L. L., (2007) "Introduction to Wireless Sensor Networks Report", University of Trento. http://dit.unitn.it/~fernand/downloads/iwsn.pdf

[16] Siahaan, I. and Fernandes, L. (2008), "Secure Routing in Wireless Sensor Networks", University of Trento. http://dit.unitn.it/~fernand/downloads/IWSNSlides.pdf

[17] Zia, T. A., (2008), "A Security Framework for Wireless Sensor Networks". http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf

[18] Heinzelman, W., Kulik, J. & Balakrishnan, H., (1999) "Adaptive protocols for information dissemination in wireless sensor networks", *The Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99)*, Seattle, WA.

[19] Anipindi, K., (2002) "Routing in Sensor Networks", University of Texas at Arlington Arlington, TX-76019. http://crystal.uta.edu/~kumar/cse6392/termpapers/Kalyani_paper.pdf

[20] Intanagonwiwat, C., Govindan, R. & Estrin, D., (2003) "Directed Diffusion for Wireless Sensor Networking", *IEEE/ACM Transaction on Networking*, VOL. 11, NO. 1.

[21] Ye, F., Chen, A., Lu, S. and Zhang, L., (2001) "A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks", *Proceedings of the 10th IEEE International Conference on Computer Communications and Networks (ICCCN'01)*.

[22] Braginsky, D. and Estrin, D., (2002) "Rumor Routing Algorithm For Sensor Networks", *First Workshop on Sensor Networks and Applications (WSNA)*, Atlanta, GA, pp. 1-12.

[23] Heinzelman, W. R., Chandrakasan, A. and Balakrishnan, H., (2000) "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", *Proceedings of the 33rd International Conference on System Sciences (HICSS '00)*, pp. 1-10.

[24] Lindsey, S., Raghavendra, C., (2002) "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", *IEEE Aerospace Conference Proceedings*, Vol. 3, 9-16 pp. 1125-1130.

[25] Manjeshwar, A., and Agrawal, D. P., (2002) "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks", *In 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing (WPIM 2002)*, p. 195b.

[26] Khan, N. M., Ali, I., Khalid, Z., Ahmed, G., Kavokin A. A. and Ramer R., (2008) "Quasi Centralized Clustering Approach for an Energy-efficient and Vulnerability-aware Routing in Wireless Sensor Networks", *HeterSanetACM*, p. 67-72.

[27] Satapathy, S.S. and Sarma, N., (2006) "TREEPSI: tree based energy efficient protocol for sensor information", *Wireless and Optical Communications Networks, IFIP International Conference*.

[28] Huang, K., Yen, Y. and Chao, H., (2007) "Tree-Clustered Data Gathering Protocol (TCDGP) for Wireless Sensor Networks", *Future generation communication and*

networking (fgcn 2007), Volume: 2, page(s): 31-36.

[29] Xu, Y., Heidemann, J. and Estrin, D., (2001) "Geography-informed energy conservation for ad hoc routing", *The Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_01)*, Rome, Italy.

[30] Shah, R. C. and Rabaey, J., (2002) "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", *IEEE Wireless Communications and Networking Conference (WCNC)*, Orlando, FL.

[31] Manjeshwar, A. and Agarwal, D. P., (2002) "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks", *Parallel and Distributed Processing Symposium, Proceedings International*, pp. 195-202.

[32] Younis, M., Youssef, M. and Arisha, K., (2002) "Energy-aware routing in cluster-based sensor networks, *The Proceedings of the 10th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002)*.

[33] Ye, F., Luo, H., Cheng, J., Lu, S. and Zhang, L., (2002) "A Two-tier data dissemination model for large-scale wireless sensor networks", *The proceedings of ACM/IEEE MOBICOM*.

[34] Rodoplu, V. and Ming, T.H., (1999) "Minimum energy mobile wireless networks", *IEEE Journal of Selected Areas in Communications*, 17 (8), pp. 1333–1344.

[35] Li, L. and Halpern, J. Y., (2001) "Minimum energy mobile wireless networks revisited", *The Proceedings of IEEE International Conference on Communications (ICC_01)*, Helsinki, Finland.

[36] Yu, Y., Estrin, D., Govindan, R., (2001) "Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks", *UCLA Computer Science Department Technical Report*, UCLA-CSD TR-01-0023.

[37] Chen, B., Jamieson, K., Balakrishnan, H. and Morris, R., (2002) "SPAN: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", *Wireless Networks*, Vol. 8, No. 5, Page(s): 481-494.

[38] Dimitrievski, A., Stojkoska,B, Trivodaliev, K. and Davcev, D., (2006) "Securing communication in WSN trough use of cryptography", *NATO-ARW*, Suceava.

[39] Parno, B., Perrig, A. and Gligor V., (2005) "Distributed Detection of Node Replication Attacks in Sensor Networks", *Proceedings of the IEEE Symposium on Security and Privacy (S&P'05)*.

[40] Sohrabi, K. , Gao, J., Ailawadhi, V. and Potie, G. J., (2000) "Protocols for self-organization of a wireless sensor network", *IEEE Personal Communications*, pp. 16-27.

[41] Sivakumar, R., Sinha, P. and Bharghavan, V., (1998) "Core extraction distributed ad hoc routing (CEDAR) specification", *IETF Internet draft draft-ietf-manet-cedar-spec-00.txt*

[42] Sharma, S., Kumar, D. and Kumar, R., (2008) "QOS-Based Routing Protocol in WSN," *Advances in Wireless and Mobile Communications*, Volume 1, pp. 51–57, Number 1-3.