Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security issues in wireless sensor networks: A review

Rakesh Sharma*
Computer Science & Engineering
HCTM Technical Campus
Kaithal, Haryana, India

Dr. V. A. Athavle
Computer Science & Engineering
Devraj Group of Institutions
Ferozpur, Punjab,India

Pinki Sharma
Computer Science & Engineering,
HCTM Technical Campus
Kaithal, Haryana, India

Abstract*— A wireless sensor network typically consists of large number of low-cost densely deployed sensor nodes that have strictly constrained sensing, computation, and communication capabilities. Because of resource restricted sensor nodes, it is necessary to reduce the amount of information transmission so that average lifetime of sensor and thus the bandwidth consumption are improved. As wireless sensor networks are typically deployed in remote and hostile environments to transmit sensitive data, sensor nodes are in danger of node compromise attacks and security issues like data confidentiality and integrity are terribly necessary. Therefore, 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*— Security, Attacks, Wireless sensor networks, Protocols**

I. INTRODUCTION

Application specific wireless sensor network consists of lots of low-power multi-functioning sensor nodes, operative in an unattended or hostile atmosphere, with restricted process and sensing capabilities. Realization of sensor network applications needs wireless unrehearsed networking techniques. But protocols and algorithms projected for ancient unrehearsed networks don't seem to be compatible because of the distinctive options and application needs of sensor networks. Attributable to its distinctive options, sensor networks are utilized in big selection of applications in areas like health, military, home and business industries in our day to day life [14] [15] [16]. Information gathering protocols are developed for configuring the network and aggregation info from the specified atmosphere. In every spherical of the information gathering protocol, information from the nodes got to be collected and transmitted to (BS), wherever from the tip user will access the information. Sensor nodes use totally different information aggregation techniques to attain energy potency. Existing information gathering protocol may be classified into four totally different classes supported the network structure and protocol operation: flat (Flooding [40], gossip mongering [40], Directed Diffusion [18], Rumor Routing [21], SPIN [20], Energy Aware Routing [24], etc), class-conscious (LEACH [37],PEGASIS[22], TEEN[23], QCCA[4], TREPSI[11], TCDGP[6], APTEEN[25], SOP[26], TTDD[27], etc), location (GAF[33], MECN [41], SMECN[34], GEAR[35], SPAN[28], etc) based mostly routing protocols and network flow or quality of service (QoS) aware routing (SAR[36], CEDAR[42], SPEED[5] etc). As WSN is generally used for gathering application specific info from the encircling atmosphere, it's extremely essential to shield the sensitive information from unauthorized access. WSNs are susceptible to security attacks because of the published nature of radio transmission. Sensor nodes may be physically captured or destroyed by the enemies. The uses of sensor network in varied applications stress on secure routing. Varied protocols are projected for routing and information gathering however none of them are designed with security as a goal. The resource limitation of sensor networks poses nice challenges for security. As sensor nodes are with terribly restricted computing power, it's troublesome to supply security in WSN victimization public-key cryptography [1]. Thus most of the projected security solutions for WSN are supported bilaterally symmetrical key cryptography. During this paper we've got reviewed feasible attacks on WSN generally moreover as attacks on specific WSN information gathering remainder of the paper is organized as follows. Section a pair of provides general summary of various security problems. Section three elaborates feasible attacks against WSN generally. In section four explores existing WSN information gathering protocols and security threats on them and at last section concludes the paper.

II. SECURITY PROBLEMS IN WSN

A. Attack and assailant

An attack may be outlined as an endeavour to realize unauthorized access to a service, a resource or info, or to decide to compromise integrity, availableness, or confidentiality of a system. Attackers, intruders or the adversaries' are is creator of an attack. The weakness in a very system security style, implementation, configuration or limitations that might be exploited by attackers is understood as vulnerability or flaw. Any circumstance or event (such because the existence of an assailant and vulnerabilities) with the potential to adversely impact a system through a security breach is named threat and therefore the likelihood that an assailant can exploit a specific vulnerability, inflicting hurt to a system plus is understood as risk

B. Security needs

A sensor network could be a special variety of unrehearsed network. Thus it shares some common property as electronic network. The protection needs [3] [7] [8] [14] of a wireless sensor network may be classified as follows:

• Authentication: As WSN communicates sensitive information that helps in several necessary choices creating. The receiver must make sure that the information utilized in any decision-making method originates from the proper supply. Similarly, authentication is critical throughout exchange of management info within the network.

• Integrity: Information in transit may be modified by the adversaries. Information loss or harm will even occur while not the presence of a malicious node because of the tough communication atmosphere. Information integrity is to make sure that info isn't modified in transit, either because of malicious intent or out of the blue.

• Information Confidentiality: Applications like police work of data, industrial secrets and key distribution got to suppose confidentiality. The quality approach for keeping confidentiality is thru the employment of secret writing.

• Information Freshness: Even though confidentiality and information integrity are assured, we tend to additionally got to make sure the freshness of every message. Information freshness suggests that the information is recent, and it ensures that no previous messages are replayed. To make sure that no previous messages replayed a time stamp may be additional to the packet.

• Availability: sensor nodes could run out of battery power because of excess computation or communication and become inaccessible. It should happen that an assailant may jam communication to form sensor(s) inaccessible. The necessity of security not solely affects the operation of the network, however is also extremely necessary in maintaining the supply of the network.

• Self-Organization: A wireless sensor network believes that each sensor node is freelance and versatile enough to be self-organizing and self-healing per totally different problem environments. Because of random preparation of nodes no fastened infrastructure is offered for WSN network management. Distributed sensor networks should self-organize to support multi-hop routing. They have to additionally self organized to conduct key management and building trust relation among sensors.

• Time Synchronization: Most sensor network applications suppose some type of time synchronization. So as to conserve power, a private sensor's radio is also turned off sporadically.

• Secure Localization: The sensor network usually wants location info accurately and mechanically. However, an assailant will simply manipulate non secured location info by news false signal strengths and replaying signals, etc.

C. Security categories

Attacks on the computer system or network may be generally classified [39] as interruption, interception, modification and fabrication.

• Interruption is an attack on the supply of the network, for instance physical capturing of the nodes, message corruption, insertion of malicious code etc.

• Interception is an attack on confidentiality. The sensor network may be compromised by somebody to realize unauthorized access to sensor node or information hold on inside it.

• Modification is an attack on integrity. Modification means that an unauthorized party not solely accesses the information however tampers it, for instance by modifying the information packets being transmitted or inflicting a denial of service attack like flooding the network with false data.

• Fabrication is an attack on authentication. In fabrication, somebody injects false information and compromises the trustiness of the knowledge relayed.

D. Threat models

Threats in sensor networks [17] may be classified as sensor-class (mote-class) assailants and laptop computer class attacker. Another classification may be created as external threats and internal threats. Stuff category attackers are also sensors with similar capabilities as sensor network. These sorts of attackers will jam the link in its immediate locality. An assailant with laptop-class devices have larger battery power, a lot of capable central processor, a high-energy sender, or a sensitive antenna and therefore they'll have an effect on way more than an assailant with solely normal sensor nodes. One laptop-class assailant could be able to snoop on a complete network. External threats could cause passive eavesdropping on information transmissions, moreover as will be injecting false information into the network to consume network resources and lift Denial of Service (DoS) attack. Whereas within assailant or internal threat is a licensed participant within the sensor network that has gone hostile. Corporate executive attacks is also mounted by either compromised sensor nodes running malicious code or adversaries agency have purloined the key material, code, and information from legitimate nodes and agency then use one or a lot of laptop-class devices to attack the network.

E. Layering-based attacks and manageable security approach

Though there's no such customary bedded design of the communication protocol for wireless sensor network, here we've got summarized doable attacks and their security answer approaches in several layers with relation to ISO OSI layer within the table-1 [3][9].

TABLE I
LAYERING-BASED ATTACKS AND FEASIBLE 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

III. ATTAINABLE ATTACKS AGAINST WSN

Most of the routing protocols projected for unrehearsed and sensor network don't seem to be designed to handle security connected problems. Thus there's lots of scope for attacks on them. Totally different achievable attacks [2][8][10][12][13][19][29][30][31][38] on the flow of data and management information may be classified as follows:

- Spoofed, altered, or replayed routing info
- 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

A. Spoofed, altered, or replayed routing info

This is the foremost common direct attack against a routing protocol. This attack targets the routing info changed between the nodes. Adversaries is also able to produce routing loops, attract or repel network traffic, extend or shorten supply routes, generate false error messages, partition the network, and increase end-to-end latency. The quality answer for this attack is authentication. i.e., routers can solely settle for routing info from valid routers.

B. Selective forwarding attack

Multi-hop mode of communication is usually most well-liked in wireless sensor network information gathering protocols. Multi-hop networks assume that collaborating nodes can dependably forward and receive messages. But a malicious node could refuse to forward sure messages and easily drop them, making certain that they are not propagated any longer. This attack may be detected if packet sequence numbers are checked properly and endlessly in a very conjunction free network. Addition of knowledge packet sequence variety in packet header will scale back this attack.

C. Sinkhole attack

By sinkhole attack, somebody tries to draw in nearly all the traffic from a specific space through a compromised node. A compromised node that is placed at the centre of some space creates an outsized "sphere of influence", attracting all traffic destined for a base station from the sensor nodes. The assailant targets an area to make depression wherever it will attract the foremost traffic, presumably nearer to the bottom station so the malicious node might be perceived as a base station. The most reason for the sensor networks prone to depression attacks is because of their specialized communication pattern. It's going to be very troublesome for somebody to launch such an attack in a very network wherever each try of neighbouring nodes uses a novel key to initialize frequency hopping or unfold spectrum communication. Sinkholes are troublesome to defend in protocols that use publicized info like remaining energy or an estimate of end-to-end irresponsibleness to construct a routing topology as a result of this info is tough to verify.

D. *Sybil attack*

Most protocols assume that nodes have one distinctive identity within the network. In a very Sybil attack, an assailant will seem to be in multiple places at identical time. This may be convincing by making faux identities of nodes settled at

the sting of communication vary. Multiple identities may be occupied inside the sensor network either by fabricating or stealing the identities of legitimate nodes. Sybil attacks will create a big threat to geographic routing protocols. Location aware routing usually needs nodes to exchange coordinate info with their neighbours to construct the network. Thus it expects nodes to be gift with one set of coordinates, however by victimization the Sybil attack somebody will ‘‘be in additional than one place at once’’. Since identity fraud ends up in the Sybil attack, correct authentication will defend it.

E. Wormholes attack

In this attack somebody might win over nodes agency would unremarkably be multiple hops from a base station that they are just one or two hops away via the hole. The best case of this attack is to possess a malicious node forwarding information between two legitimate nodes. Wormholes usually win over distant nodes that they are neighbours, resulting in fast exhaustion of their energy resources. Somebody set near a base station is also able to utterly disrupt routing by making a well-placed hole. Wormholes are effective even though routing info is genuine or encrypted. This attack may be launched by insiders and outsiders. This may produce a depression since the somebody on the opposite aspect of the hole can by artificial means give a prime quality route to the bottom station, probably all traffic within the close space are drawn through her if alternate routes are considerably less enticing. Once this attack is plus selective forwarding and therefore the Sybil attack it is terribly troublesome to notice. A lot of usually, wormholes may be accustomed exploit routing race conditions. A routing race condition generally arises once a node takes some action supported the primary instance of a message it receives and after 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 will stop this by avoid routing race conditions. The answer needs clock synchronization and correct location verification, which can limit its pertinence to WSNs.

F. Hello flood attack

Many protocols need nodes to broadcast hullo packets for neighbour discovery, and a node receiving such a packet could assume that it is inside (normal) radio vary of the sender. A laptop-class assailant with giant transmission power might win over each node within the network that somebody is its neighbour, so all the nodes can answer the hullo message and waste their energy. The results of a hello flood are that each node thinks the assailant is inside one-hop radio communication vary. If the assailant after advertises low-priced routes, nodes can decide to forward their messages to the assailant. Protocols that depend upon localized info exchange between neighbouring nodes for topology maintenance or flow management also are subject to the current attack. Hello floods may also be thought of as unidirectional, broadcast wormholes. We will stop this attack by validate the bi-directionality of native links before victimization them is effective if the assailant possesses identical reception capabilities because the sensor devices. Otherwise by victimization genuine broadcast protocols.

G. Acknowledgement spoofing

Several sensor network routing algorithms suppose implicit or express link layer acknowledgements. Because of the inherent medium, somebody will spoof link layer acknowledgments for “overheard” packets self-addressed to neighbouring nodes. Protocols that select subsequent hop supported irresponsibleness problems are prone to acknowledgments spoofing. This leads to packets being lost once travelling on such links. The goal includes convincing the sender that a weak link is robust or that a dead or disabled node is alive. Since packets sent on weak or dead links are lost, somebody will effectively mount a selective forwarding attack victimization acknowledgement spoofing by encouraging the target node to transmit packets on those links. Acknowledgement spoofing attacks may be prevented by victimization sensible secret writing techniques and correct authentication for communication.

H. Sniffing attack

Sniffing attack could be an ideal of interception or listen-in channel attack. During this attack somebody node is placed within the proximity of the sensor grid to capture information. The collected information is transferred to the trespasser by some means that for any process. This sort of attack won't have an effect on the traditional functioning of the protocol. An out of doors assailant will lunch this attack for gather valuable information from the sensors. Usually this attack is expounded to military or industrial secrets. The attack is predicated on the inherit vulnerability of the wireless networks of getting unsecured and shared medium. Sniffing attacks may be prevented by victimization correct secret writing techniques for communication.

I. Information integrity attack

Data integrity attacks compromise the information travelling among the nodes in WSN by ever-changing the information contained inside the packets or injecting false data. The assailant node should have a lot of process, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor information and by doing thus compromise the victim’s analysis. It additionally falsifies routing information so as to disrupt the sensor network’s traditional operation, presumably creating it useless. This is often thought of to be a kind of denial of service attack. This attack may be defended by adapting uneven key system that's used for secret writing or we will use digital signatures, however this needs lots of extra overhead and is troublesome to adapt in WSN.

J. Energy drain attack

WSN is battery high-powered and dynamically organized. It's troublesome or not possible to replace/recharge sensor node batteries. As a result of there's a restricted quantity of energy accessible, attackers could use compromised nodes to inject fancied reports into the network or generate great deal of traffic within the network. Fancied reports can cause false alarms that waste world response efforts, and drain the finite quantity of energy in a very battery high-powered network. But the attack is feasible provided that the intruder's node has enough energy to transmit packets at a relentless rate. The aim of this attack is to destroy the sensor nodes within the network, degrade performance of the network and ultimately split the network grid and consequently lead of a part of the sensor network by inserting a brand new Sink node. To reduce the harm caused by this attack fancied reports ought to be born en-route as early as doable.

K. Black-hole attack

The part attack positions a node in vary of the sink and attracts the complete traffic to be routed through it by advertising itself because the shortest route. Somebody drops packets returning from specific sources within the network. This attack will isolate sure nodes from the bottom station and creates a separation in network property. This attack is simpler to notice than depression attack. This attack usually targets the flooding based mostly protocols. Another attention-grabbing variety of attack is orientating. In a very orientating attack, the assailant appearance at network traffic to deduce the geographic location of crucial nodes, like cluster heads or neighbours of the bottom station. The assailant will then physically disable these nodes. This ends up in another variety of part attack. This attack aims to dam the traffic to the sink and to supply a more robust ground for feeding alternative attacks like information integrity or sniffing. This attack may be prevented if we will limit malicious node to hitch the network. Network setup section ought to be meted out in a very secure manner.

L. Node replication attack

This is an attack wherever assailant tries to mount many nodes with same identity at totally different places of the prevailing network. There are two strategies for mounting this attack. In 1st technique the assailant captures one node from the network and creates a twin of a captured node and mounts in several places of the network. In second technique assailant could generate a false identification of a node then makes clone out of this node and mounts in several places of the network. These mounted clone nodes tries to generate false information to disrupt the network. Node replication attack is totally different kind Sybil attack. In Sybil attack one node exists with multiple identities however in node replication attack multiple nodes gift with same identity. Therefore in Sybil attack an assailant will succeed by mounting solely one node wherever as node replication attack needs a lot of nodes to be mounted throughout the network this will increase the prospect of detection. This attack may be avoided if we tend to centrally calculate the information gathering path by the baccalaureate then multiple place prevalence of the node may be detected. The opposite thanks to notice the attack is validate the identities (authentication) of nodes by a trustworthy node.

IV. DOABLE ATTACKS ON EXISTING PROTOCOLS

Depending on the specification and data used whereas taking routing call, routing protocol in WSNs may be classified into flat-based routing, hierarchical-based routing, location-based routing, and network flow or quality of service (QoS) aware routing. A number of the protocols follow the characteristics of quite one category, attributable to that classification might not be utterly distinct and that they could overlap on one another. For instance one in every class-conscious protocol PEGASIS that is assessed as class-conscious protocol additionally uses location info for forming a sequence like path of the nodes. Rather than classify them beneath location based mostly routing protocol, we tend to most well-liked to classify them beneath class-conscious based mostly routing the communication pattern they follow.

A. Flat based mostly routing protocol

Flat routing assumes that nodes have uniform responsibility within the network. Sensor nodes wishing on some wanting flooding mechanism to unfold question request within the network for gathering info. As a large variety of nodes are deployed in WSN, information is sometimes transmitted from each sensor node with vital redundancy. This sort of protocols consumes a lot of energy than others and thus so as to reduce energy consumption, nodes mixture information throughout transmission. Protocols that will be classified beneath this class are: Flooding [40], gossip mongering [40], Directed Diffusion [18], SPIN [20], Rumor Routing [21], The Minimum Cost Forwarding Protocol [32], Energy Aware Routing [24] etc.

1) Doable attacks on flat based mostly routing protocols

In flat routing nodes got to exchange hullo packets among themselves to get neighbours for charring out digital communication. Somebody node could be a part of throughout neighbour discovery section and win over neighbour node to be the closest to them, thus on forward information towards it and therefore implant depression attack. Within the neighbour discovery section of the flat routing protocol somebody nodes could be a part of the network with false node identity and seem with multiple identity to its neighbour resulting in Sybil attack. In flat routing all communication happens to be neighbour-to-neighbour. With the assistance of two somebody node assailant will produce tunnel within the network, this is often doable by convincing nodes as neighbours'' of somebody node. This helps to introduce Wormhole attack within the network. Exchange hullo packet provides a more robust ground for mounting hullo flood attack. Sniffing attack could be a common attack which may mount with success with less effort. If somebody placed

close to the bottom station it will simply capture the information while not distressful the network. just in case of the flat routing most of the protocol follows information flooding technique, this provides a more robust ground for the sniffing attack to be mounted. Multi-path information delivery ends up in straightforward information integrity attack. If somebody changes the information in one path then it puts a matter mark on the irresponsibleness of the information. During this attack assailant must determine the trail of communication and place somebody therein path to alter the information. Somebody will generate false information or question by connation the network. Once a node responds to those wrong information or question, leads them to suffer from the energy drain attack. Flat routing is a lot of prone to this sort of energy drain attack because of there pattern of communication. In flat routing protocol, somebody node placed close to the bottom station will attract entire network traffic to mount the part attack. Assailant will mount somebody nodes with same id or false id in several place of the network. These nodes generate the false information and disrupt the information communication. It puts a matter mark on information integrity additionally. Flat routing suffers from information integrity attack as node may be mounted in impulsive position within the network and includes them within the network in neighbour discovery section.

2) Attacks might not be applicable on flat based mostly routing protocols

As most of flat based mostly routing protocols follow multi-path information delivery or information flooding technique, we tend to expect no-hit information delivery at the bottom station even though there's some faulty path. thus Spoofed, altered or replayed routing info attack moreover as Selective forward attack don't seem to be fruitful for the flat based mostly routing protocols. Sometimes to make sure irresponsibleness acknowledgement is predicted for every no-hit information delivery. Just in case of flat routing most of the protocols, node floods information with in its neighbourhood. Thus information delivery is predicted while not reckoning on the acknowledgement and therefore acknowledgement spoofing attack might not achieve success here.

B. Class-conscious protocols

In hierarchical-based routing, nodes within the network play totally different roles in several instance of your time. The class-conscious routing conserves energy by adopting multi hop communication, information aggregation and fusion in WSN. During this design low energy nodes perform the sensing and human activity in a very short varies wherever as higher energy nodes method and send the knowledge in long vary. Class-conscious routing will increase overall system measurability, lifetime, and energy potency of WSN. It additionally reduces variety of transmissions. Class-conscious routing is sometimes a two-phase routing wherever one section is employed to pick out the cluster-heads and therefore the alternative one is employed for routing. Few protocols returning beneath this class are LEACH [37], PEGASIS [22], TEEN [23], APTEEN [25], SOP [26], TREPSI [11], TCDGP [6], QCCA [4], TTDD [27], etc.

1) Doable attacks on class-conscious protocols

In case of class-conscious routing, constellation could depend upon communication vary of the nodes, location info, distance between the nodes and remaining battery power. Somebody will manipulate these parameters to mount spoofed, altered, or replayed routing info attack and attract the network towards it to make a depression. This sink hole could change into part if it absorbs the information utterly. These protocols transmit information in multi-hop thus intermediate nodes take the responsibility of knowledge aggregation/fusion and forward data to higher level. Somebody agency joins the network in setup section will by selection forward information to higher level and alters the info to guide data integrity attack. In class-conscious based mostly routing nodes collaborate among themselves to create the multi-hop routing. For this node collaboration they have to grasp their node identities. This provides a more robust ground for the somebody nodes to seem with multiple identities within the network and create Sybil attack trivial. Assailant will mount somebody nodes with same id in several place of the network and actively be a part of the network. These nodes generate the false information and disrupt the information communication. The protocol wherever digital communication path is computed centrally by the bottom station (TREEPSI) will simply detect/avoid this attack. Nodes try and collaborate with its nearest neighbour which may forward the information to the bottom station. Somebody will win over nodes as nearest neighbour and force them to forward information through it. Finally this somebody could replay this information at another a part of the network by making tunnel with the assistance of somebody nodes. This makes whole attack trivial in class-conscious routing. Neighbour discovery could be a very important a part of class-conscious routing protocol. For neighbour discovery hullo packets got to be changed between the nodes. A laptop computer category somebody will take the advantage of this and flood hullo packets within the network to win over the nodes as its neighbour. With the assistance of this somebody energy drain attack may be mounted. Even though class-conscious routing follows multi-hop, it depends node to node communication moreover. Thus whenever a node sends information to a different node, it expects an acknowledgement from the receiving node. Somebody nodes could take the advantage of this and send false acknowledgement for weak and dead nodes to win over the network as alive. Leader nodes take the responsibility of forwarding information to the bottom station. They transmit with decent power to achieve the bottom station. Thus if somebody is placed close to the bottom station it will simply capture information and send it to trespasser base station for any process.

C. Location-based protocols

In location based mostly routing, sensor nodes are self-addressed by their locations. Most of the routing protocols conserve energy by transmission to the nodes inside neighbour space. The gap between neighbour nodes may be

calculable on the idea of incoming signal strengths or accurately with the assistance of GPS. Coordinates of neighbour nodes may also be obtained by exchanging location info between neighbours. Here entire network is split into tiny grids. Just in case there's no activity in a very grid, nodes inside that grid enter in to sleep mode to conserve energy. If the region to be perceived is understood, victimization the situation of sensors, the question may be subtle solely to it explicit region which can eliminate the quantity of transmission considerably. Location based mostly routing protocols are well applicable to sensor networks wherever there is less or no quality. Some example of the on top of kind is MECN [41], SMECN [34], GAF [33], GEAR [35] and SPAN [28] etc.

1) Doable attacks on location-based protocols:

To save energy, some location based mostly schemes demand that nodes ought to attend periodic sleep if there's no activity. Somebody node will take the advantage of this and win over nodes to travel to sleep mode. This leads sure region inaccessible to base station. Assailant succeeds to mount part and selective forwarding attack. Somebody nodes will generate false location info and be a part of the network to mount Sybil attack. During this variety of protocols nodes in a very grid communicate with each alternative and with other grids. This needs hullo packet exchange between neighbours. Somebody could take the advantage of this to mount hullo flood attack. Grids communicate with the assistance of co-coordinator node. Somebody takes the advantage of this to make a hole and tunnels information from one half to a different a part of the network. If an assailant places somebody close to the desired grid then it will capture the information of that specific grid. It's higher to position somebody close to the bottom station wherever it will capture information from all the regions. Primarily during this class of protocols question is placed to sure region supported the situation info. Thus somebody will generate false question and send to the targeted space of the network. The nodes gift during this region responds to the question and drains their battery. Kind of like the case of class-conscious routing whenever a node sends information it expects acknowledgement. Somebody nodes could take the advantage of this and send false acknowledgement for weak and dead nodes to win over the network as alive.

2) Attacks not applicable on location-based protocols

In location based mostly routing protocol most of the protocol use GPS to search out the situation of the node. It's assumed that location info is correct because of use of GPS. On the idea of this info network grids are shaped to hold out communication. Thus it's troublesome for an assailant to mount spoofed, altered or replayed routing info attack, depression attack and node replication attack.

D. Network flow and QoS-aware protocols

In QoS-based routing protocol, route setup is intended as a network flow drawback. The sensor network methods are obtained by levelling energy consumption and information quality. The network must satisfy sure QoS metrics, e.g., delay, energy, bandwidth, etc. once delivering information to the baccalaureate. To avoid single route failure in QoS-based routing protocol, multi-path approaches moreover as localized path restoration schemes are used. A number of protocols categorized beneath this class are SAR [36], CEDAR [42], SPEED [5] etc.

1) Doable attacks on network flow and QoS-aware protocols

In these protocols network methods setup is predicated in spite of everything between energy consumption and information quality. Thus somebody will generate false energy info and information measure to draw in nodes to incorporate her within the path and send information through it. This helps to make sink hole within the network. Assailant will ultimately convert this sink hole to part. Like depression worm hole may be created by generating false messages. Once the depression attack is mounted with success one will create selective forward attack trivial. So as to construct routing path, nodes got to share info like energy and information quality. Another purpose is that, these protocols do localized path restoration to take care of routing path that hullo packet got to be changed between the nodes. Thus somebody will take the advantage of these to mount the hullo flood attack. Information transmission is multi-hop mode in network flow and QoS aware protocols. For irresponsibleness in digital communication acknowledgement is needed. AN assailant takes the advantage of this and may mount acknowledgement spoofing attack to bias the network. The assailant will place somebody close to the network grid to capture information and say any process to the trespasser base station Multi-hop information delivery ends up in straightforward information integrity attack. Any intermediate compromised node wills modification the information to guide data integrity attack. Multiple somebody nodes may be mounted in several place of the network with same identity. This node replication attack will facilitate the assailant to empty the battery of neighbour nodes by generating false information and routing info.

2). Attacks not applicable on network flow and QoS-aware protocols:

Since most of those protocols follow multi-path approach and localized path restoration schemes thus we tend to expect it's troublesome for the some body to bias routing. If some body node tries to exist with multiple identities may be simply detected because of localized path restoration. The summarized report of the various attacks on the protocols is given below in table a pair of. A tick mark entry within the table indicates that a protocol returning beneath the category of the protocol could suffer from the corresponding attack, wherever as a cross mark indicates that the protocol is immune from the attack. In our intensive study we tend to found that class-conscious protocols suffer from all the attacks. But individual protocols classified beneath class-conscious cluster might not suffer from all the attacks. Like that location

based mostly protocols will defend a lot of attacks than alternative protocols. However these protocols have downside of victimization of GPS. This might cause complicacy in style moreover as costly sensor nodes.

TABLE II
ATTACKS AND PROTOCOLS

ATTACK	PROTOCOL
Spoofed, altered, or replayed routing information	Hierarchical protocol.
Selective forward	Hierarchical, Location-Based, Network flow and QoS-aware protocol.
Sink hole	Flat Based Routing, Hierarchical, Network flow and QoS-aware protocol.
Sybil	Flat Based Routing, Hierarchical, Location-Based protocol.
Worm Hole	Flat Based Routing, Hierarchical, Location-Based, Network flow and QoS-aware protocol.
HELLO flood	Flat Based Routing, Hierarchical, Location-Based, Network flow and QoS-aware protocol.
Acknowledgement spoofing,	Hierarchical, Location-Based, Network flow and QoS-aware ptotocol.
Sniffing	Flat Based Routing, Hierarchical, Location-Based, Network flow and QoS-aware protocol.
Data integrity	Flat Based Routing, Hierarchical Network flow and QoS-aware protocol.
Energy drain	Flat Based Routing, Hierarchical, Location-Based, Network flow and QoS-aware protocol.
Black hole	Flat Based Routing, Hierarchical, Location-Based, Network flow and QoS-aware protocol.
Node replication attack	Flat Based Routing, Hierarchical, Network flow and QoS-aware protocol.

V. CONCULSION

This paper covers totally different security problems in wireless sensor network generally and created an intensive study of various threats related to existing information gathering protocols. As these protocols don't seem to be designed taking security problems under consideration, most of them are liable to differing types of attacks. Even a number of the protocols are appears to be susceptible to most of the attacks. Equally some attacks like hello flood, Acknowledgement spoofing and sniffing may be utilized by the adversaries to have an effect on most of the protocols.

REFERENCES

[1] Mohanty P., Panigrahi S., Sarma N And Satapathy S. S.(2010)" Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey" JTAIT PP-14-27,

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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

[10] Committee on National Security Systems (CNSS), (2006) National Information Assurance Glossary, NSTISSI,No. 4009. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

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

[12] 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).

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

[14] 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.

[15] 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.

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

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

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

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

[20] Anipindi, K., (2002) "Routing in Sensor Networks", University of Texas at Arlington Arlington, TX-7601 http://crystal.uta.edu/~kumar/cse6392/termpa pers/Kalyani_paper.pdf

[21] 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.

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

[23] 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 Wireles Networks and Mobile Computing (WPIM 2002), p. 195b.

[24] 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.

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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).

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

[34] 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.

[35] 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.

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

[37] 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.

[38] 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.

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

[40] 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.

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

[42] 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

