ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

Towards Efficient Wireless Sensor Networks: A Survey on Routing Factors, Routing Protocols and EN-Routing Filtering Schemes

Gopinath.D[1], Ramesh.P[2]

Research Scholar, Dept. of Computer Science, Kongu Arts and Science College, Erode, India[1]

PhD (Part Time) Research Scholar, Dept. of Computer Science, Bharathiar University, Coimbatore, India[2]

ABSTRACT: Wireless sensor networks (WSN) have lot of interest in research due to their wide range of typical application areas such as environmental, military and commercial enterprises. High efficient routing is an important issue for the design of wireless sensor network (WSN) protocols to meet the severe hardware and resource constraints. Sensor network possesses unique challenges to protocol builders, because these tiny wireless devices are often deployed in unattended environment with limited capabilities. Hence these networks are vulnerable to different types of malicious attacks. This paper surveyed the different types of attacks and security related issues in WSN. Moreover an analysis about some of the major domains namely, architecture, attacks, routing factors, routing protocols, filtering schemes.

Keywords: Wireless sensor networks, attacks, routing factors, routing protocols, filtering schemes.

I. INTRODUCTION

WIRELESS Sensor Networks (WSN) are increasingly gaining momentum in our lives. Tomorrow's healthcare systems, smart homes, power management systems will involve a large number of interconnected smart wireless (sensor) devices that will be operated and controlled by end users (a home user or an administrator). These devices have the capability to connect and interact, and provide a backbone for the future development of the "Internet of Things." In a WSN environment, the nodes might need to communicate security sensitive data among themselves and with the base station (also referred to as "sink"). The communication among the nodes might be point-to-point and/or broadcast, depending upon the application. These communication channels, however, are easy to eavesdrop on and are easy to manipulate, raising the very real threat of the so-called man-in-the-middle attacker. A fundamental task, therefore, is to secure these communication channels.

A. Motivation for Secure Initialization

A number of so-called "key predistribution" techniques to bootstrap secure communication in a WSN have been proposed, e.g., [5], [22], [11], [27], [15]. However, all of these techniques assume that, before deployment, sensor nodes are somehow preinstalled with secret(s) shared with other sensor nodes and/or the sink. The TinySec architecture [20] also assumes that the nodes are loaded with shared keys prior to deployment. This might be a reasonable assumption in some, but certainly not all, cases. Let us consider, for example, a user-centric application of WSN. An individual user (Bob) wants to install a sensor network to monitor the perimeter of his property; he purchases a set of commodity noise and vibration sensor nodes at certain retailers, and wants to deploy the sensor nodes with his home computer acting as the sink. Being off-the-shelf, these sensor nodes are not sold with any built-in secrets. Some types of sensor nodes might have a USB (or similar) connector that allows Bob to plug each sensor node into his computer to perform secure initialization. This would be immune to both eavesdropping and man-in-the-middle attacks. However, most sensor nodes might not have any wired interfaces, since having a special "initialization" interface influences the complexity and the cost of the sensor node. Also, note that Bob would have to perform security initialization manually and separately for each sensor node. This undermines the scalability of the approach since potentially a reasonably large number of sensor nodes might be involved.

Furthermore, keys cannot always be preloaded during the manufacturing phase, because eventual customers might not rust the manufacturer, for example, in WSNs deployed for military applications. Moreover, a WSN application might involve nodes produced by multiple manufacturers. Due to this reason, establishing preshared secrets or a PKI-based solution might be infeasible as it would require a global infrastructure involving many diverse manufacturers. We note that the problem of secure WSN initialization that we consider in this paper is very similar to the well-studied

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

problem of "wireless (two device) pairing," the premise of which is also based on the fact that the devices wanting to communicate with each other do not share any preshared secrets or a common PKI with each other [10], [3].

II. BASIC ARCHITECTURE OF WIRELESS SENSOR NETWORKS

Wireless sensor network is applied in data collection, monitoring, surveillance, and medical telemetry etc [1]. In addition to sensing, WSNs are also interested in control and activation.

There are four basic components in a sensor network, shown in figure 1: an assembly of distributed or localized sensors; an interconnecting network; a central point of information cluster; and a set of computing resources at the central point to handle data correlation, event trending, status querying, and data mining. The density of the sensor networks is always very large, for instance, in a ten square meters region more than five or six sensor nodes may be deployed. This feature of sensor networks makes it ascendant on tracking:

1) the quality of the sensed data can be more reliable;
2) the information about the tracked target can be more accrual [23, 14].

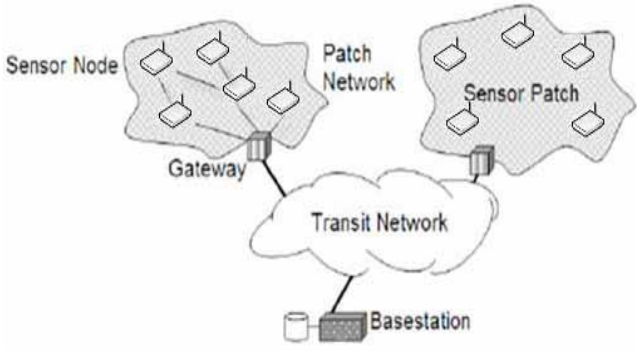

Fig.1.Wireless Sensor Network (Basic Architecture) an assembly of distributed or localized sensors; an interconnecting network; a central point of information cluster; and a set of computing resources at the central point to handle data correlation, event trending, status querying, and data mining.

An attack is an event that diminishes or eliminates a network's capacity to perform its expected function and an adversary is a person or another entity that attempts to cause harm to the network by unauthorized access or denial of service. In WSN an attacker can falsify local sensor values in the area of WSN and may be able to mislead monitors in those areas. So a sensor node is not able to communicate and coordinate with the network and it is disrupted. Attacks [29] against wireless sensor networks could be broadly considered from different levels of views.

An outside attacker is a malicious node, not part of the network, but wants to harm the network, whereas an inside attacker is the one that is inside the network authorized to access the system resources but uses them in a way not approved by the granted authorization. Remote attack can be implemented from a large distance, for instance, by emitting a high-energy signal to interrupt the communication. A passive attacker just eavesdrops or monitors the packets that are transferred in a WSN. An adversary directly influences packets in the network through active attack as the fabrication of additional packages or suppression of existing packets.

In physical layer jamming is a common attack that can be done by adversaries by knowing the wireless transmission frequencies used in WSN. The attacker who uses its radio to listen the frequency and sends his own signal interfering with the message is called as collision attacker. Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the doubt to the neighbor nodes. In Sinkhole attack adversary attracts the traffic to a compromised node. A type of attacks where a node create multiple illegitimate identities in sensor network either by fabricating or stealing the identities of legitimate nodes is called Sybil attack. In a wormhole attack an adversary records information at an origin point and retransmits the information in the neighborhood of the destination.

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. Node compromise allows the adversary to enter inside the perimeter of security. While sending the report, the information in transit may be attacked to provide wrong information base stations or sinks.

III. WSN NODE ARCHITECTURE

The backbone of WSNs lies in the ability to deploy large number of tiny nodes that assemble and configure themselves for a specific purpose. The most common application of sensor network technology is to monitor remote environments for low frequency data trends. For example, a chemical plant could be easily monitored for leaks by hundreds of sensors that automatically form a wireless interconnection network and immediately report the detection of

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

any chemical leaks. Unlike the traditional wired systems, deployment cost is set to a minimum [8]. In addition to reducing the installation costs, wireless sensor networks also have the ability to adapt dynamically to changing environments. These can respond to changes in network topologies. A wireless sensor network node consists of four major parts such as

1. Sensor unit.
2. Processing unit.
3. Energy source unit.
4. Transceiver.

Depending on the area and purpose of use, additional components might be required such as localization unit, energy harvesters, position changers and monitors as shown in Fig. 2. In many WSN applications, the deployment of sensor nodes is performed in an ad-hoc manner without proper planning or studies. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. As sensor nodes are battery powered and expected to operate and execute their duties without attendance for a long duration of time during the application, it is difficult and even impossible to change or recharge batteries for the sensor nodes [4] [8]. Despite the different objectives of sensor networks applications, the main function of wireless sensor nodes is to sense and collect information (data) from a target area, process, and transmit the information via a radio transmitter back to a command center where the underlying application resides (sink) [2] [25]. In order to achieve this task efficiently, an efficient routing protocol is needed to set up paths of communication between the sensor nodes (sources), and the command center (sink). The path selection must be such that the lifetime of the network is maximized. Due to the characteristics of the environment in which the sensor node is to operate, coupled with severe resource constraints in on-board energy, transmission power, processing capability, and storage limitations, this prompts for careful resource management and new routing protocols so as to counteract the differences and challenges

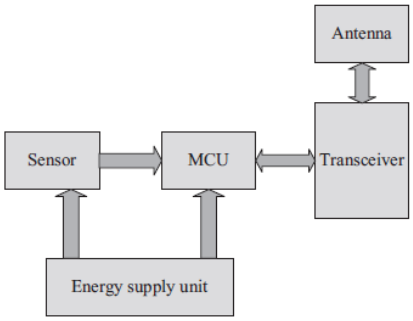

Fig. 2. WSN node architecture (In Fig wireless sensor nodes is to sense and collect information (data) from a target area, process, and transmit the information via a radio transmitter back to a command center where the underlying application resides (sink))

IV. WSNs DESIGN AND ROUTING FACTORS

A large number of research have been carried out to overcome the constraints of WSNs and also to solve the design and application issues. The characteristics of sensor networks and application requirements have direct impact on the network design issues in terms of network performance and capabilities [4]. Due to the large number of sensor nodes and the dynamics of their operating environment, these then pose unique challenges on the architectural design of sensor networks. New platforms are needed to overcome all the challenges and cover the following issues; power consumption, fault tolerance, scalability, productive cost, quality of service, data aggregation and fusion, node mobility, connectivity, security, congestion, latency, etc. Routing design is closely related to the network system architecture mode and the design of routing protocols in WSNs is influenced by many challenging factors to be addressed which are outlined and discussed below.

A. Limited energy capacity: the process of setting up routes in a network is greatly affected by energy considerations. Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a great challenge in many applications of sensor networks. Since radio transmission degrades with distance much faster than transmission in free space, it then implies that communication distance and energy consumption must be well managed. In the case of directed and multi-hop routing, directed routing would perform well enough if all sensor nodes are close to the sink, whereas multi-hop routing consumes less power than directed routing due to the fact that, sensors are usually randomly scattered in the area of deployment, though it may introduce significant overheads for topology management and MAC protocols. For applications in the battle field where it is virtually impossible to access the sensors and recharge their

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

batteries[4] [8], routing protocols design for sensor networks should be as energy efficient as possible to extend their lifetime, and hence, prolong the network lifetime without performance degradation.

B. *Node deployment:* sensor nodes deployment in WSNs is application dependent and affects the performance of the routing protocol. If nodes are randomly deployed, they need to create an infrastructure in an ad-hoc manner and organize themselves to establish paths to route the events using route discovery so as to allow connectivity and energy efficient network operation.

C. Sensor location: sensor location at the early stage of route discovery is a great challenge in the design of routing proto- cols. As most of the already proposed protocols assumes that the sensor nodes either are equipped with global positioning system (GPS) receivers or other forms of sensing the destination or sink as in [8] and [31], to learn about their locations, another challenge which has to be managed is the location of the sensors.

D. Dynamic network: sensor networks consist of three main components; sensor nodes, event, and sink. Since sensor node and sink are always assumed to be fixed or mobile, though, nodes are fixed in most of the applications, this have to support the mobility of sinks or gateways in the network. Hence, the stability of the routing data is an important design issue in addition to energy consumptions and bandwidth utilization [4] [8] [24].

E. Hardware resource constraints: sensor nodes also have limited storage and processing capacities, and hence, low computational capabilities. The hardware constraints present many challenges in the network and software protocol design for sensor networks, which have to be considered alongside with the limited energy.

F. Data aggregation and gathering: data gathering or reporting is concerned with any physical event of the sensor network. This could be event driven, query driven, or automated time driven, or both combined. Data gathering methods are highly important with respect to sensor network routing, as after receiving signal or data, the node has to transfer or route the data or information to the sink [28]. Also, since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced, which will help in energy minimization.

G. Scalability: since sensor applications may have many sensor nodes, it implies that, since the number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, it then means that routing algorithms must be scalable enough to handle and respond to the events. Abstraction and simplicity mechanism is a demanding factor, since a large amount of data is expected to be decreased to manage- able size [7].

H. Fault tolerance: the failure of a particular sensor node due to power, physical damage, or environmental interference in a network, should not in any way affect the overall network performance or task handling. In case of the failures, routing protocols should be able to generate new routes to the data collection point or sink [21].

I. Latency: latency or end-to-end delay in WSNs is an expression of how much it takes for a data packet to get from one node to the sink or vice versa. This is the measure of either one-way (the time it takes for the source to send a packet to the sink), or round-trip (the one-way latency from source to sink and from sink back to the source). Data aggregation and multi-hop relays can affect latency [30] [19].

V. ROUTING PROTOCOLS IN WSNS

Determining which set of intermediate nodes are to be selected to form a data forwarding path between the source and the destination is the principal task of the routing algorithm. The computational complexity and the differences in the way data are forwarded from the nodes to the sink, leads to classifying the routing protocols as either classical or swarm intelligence based, and or data-centric, hierarchical, location based, network flow and quality of service (QoS) awareness [2]. Shown in Table I is the taxonomy of the routing protocol classification in wireless sensor networks. The numbers in parentheses indicate the section numbers for easy and quick referencing. Routing protocols could also be classified based on path establishment. Using the path establishment classification, routing path can be established in one of the three ways: proactive, reactive or hybrid.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

TABLE II

TAXONOMY OF ROUTING PROTOCOL CLASSIFICATION IN WIRELESS SENSOR NETWORKS.

	Classical based routing protocols	**Swarm intelligence based routing protocols**
Data-centric	SPIN (5.1.3) F&G (5.1.1), DD (5.1.2), EAR (5.1.5), RR (5.1.6) CADR (5.1.7), COUGAR (5.1.9), EAD (5.1.10) GBR (5.1.4), ACQUIRE (5.1.8)	CRP (6.1.2) PEADD (6.1.1)
Location based	GEAR (5.2.2), TBF (5.2.5), EAGRP (5.2.6) GAF (5.2.1), MECN (5.2.3), SMECN (5.2.4) LEACH (5.3.1), SOP (5.3.3)	 SC (6.2.1) SDG (6.3.1), EBAB (6.3.2), ACO-C (6.3.3), ACALEACH (6.3.4) MACS (6.3.5)
Hierarchical	TEEN (5.3.4) PEGASIS (5.3.2), APTEEN (5.3.5), HEED (5.3.6) EAR-CSN (5.3.7), BCEE (5.3.8) MLDG (5.4.1)	AntChain (6.3.6), PZSWiD (6.3.7), ACMRA (6.3.8), ACMT (6.3.9) ACLR (6.3.10), MSRP (6.3.11), JARA (6.3.12), ACOLBR (6.3.13), ACO-RC (6.3.14) EEABR (6.4.1), AR & IAR (6.4.5), iACO (6.4.7), MO-IAR (6.4.9) Ant-aggregation (6.4.10), ASAR (6.4.11), BABR (6.4.12) ACO-EAMRA (6.4.13), EAQR (6.4.14), IACR (6.4.15)
Network flow and QoS aware	AODV (5.4.8) SAR (5.4.2), MLER (5.4.3), SPEED (5.4.4), EAQSR (5.4.5), MCBR (5.4.6)	E-D ANTS (6.4.4), Beesensor (6.4.6), ACO-QoSR (6.4.8), QDV (6.4.16) FF (6.4.2), FP (6.4.3), ANTSENSNET (6.4.17)

A. Swarm intelligence routing protocols: these are protocols that depend on the collective behaviour of biological species (e.g., ants) to provide a natural model for distributive problem solving without any extra central control or coordination. The basic concepts of the protocols are self-organization, which include positive feedback, negative feedback, fluctuation amplification, and multiple interactions. Consider the ant colony as an example to illustrate these concepts. The action of disposing pheromone is a positive feedback mechanism to recruit more ants such that more pheromones are disposed on the shorter path. However, the evaporation of pheromone is a negative feedback to reduce the pheromone level. In this way, the shortest paths to the food source can be found accordingly. Moreover, stigmergy is defined as the indirect communication used by ants in nature to coordinate their joint problem solving activities. Ants achieve stigmergic communication by laying a chemical substance called pheromone [30] that induces changes in the environment which can be sensed by other ants.

1. Multi-sink swarm-based routing protocol

MSRP is a routing protocol for sensor networks which is self organized, fault tolerant and environmental adaptable. The protocol is inspired by slime mold organisms. The organism finds their advantage in the ability to organize themselves in clusters using pheromone generation and evaporation. The protocol organizes data traffic towards the sink by adopting the gradient concept while showing autonomy and fault tolerance. The algorithm uses OMNET++ in the evaluation of its performances, signalling overhead, and adaptation to changes in environment.Fig3 shows the signalling process phases.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

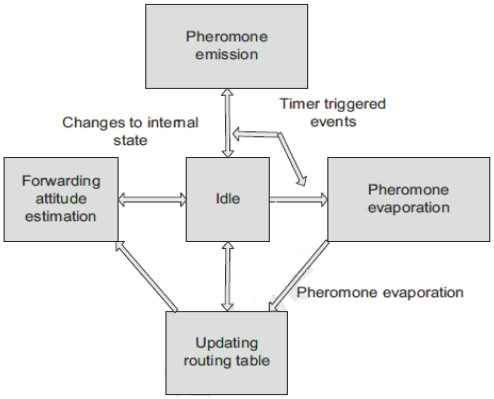

Fig. 3. Signalling process phases of multi-sinks warm based routing (MSRP is a routing protocol for sensor networks which is self organized, fault tolerant and environmental adaptable. The protocol organizes data traffic towards the sink by adopting the gradient concept while showing autonomy and fault tolerance)

B. Classical routing protocols: classical routing protocols are those protocols which were primarily designed for Mobile adhoc Network (MANET), but have now been used for WSN. Though suited for WSN applications it still has a lot of challenges like scalability and robustness. Classical routing methods are employed by a sensor node or a base station independently.

1. Classical based data-centric routing protocols

Broadcast and unicast are two operations that sensor nodes use to communicate with each other. In data centric routing, the sink sends queries to certain regions and waits for data from the sensors located in that area. Data centric utilizes data aggregation in relaying of data, which when data are measured or arrive from a neighbor, the sensor needs to decide whether or not they are important enough to forward them. The coding techniques used need to minimize the number of forwarded bits. The new data may also be combined with other received data, in order to minimize the number of bits to forward. SPIN which happen to be the first data-centric protocol, utilizes negotiation between nodes in the sensor networks so as to eliminate information that are redundant, and as such save energy.

2. Location-based protocols

In routing, some of the protocols for sensor networks require location information for the nodes; the nodes are addressed by means of their locations. The information of their respective location is needed so as to aid in the calculation of distance between two nodes, and be able to diffuse a query to a particular region, hence eliminating the number of transmission. This in turn helps in the estimation of the energy consumption.

3. Hierarchical protocols

A hierarchical protocol is an approach to the balance between scalability and performance. In hierarchical routing, energy consumption of sensor nodes is drastically minimized when the sensor nodes are involved in multi-hop communication in an area of cluster and performing data aggregation and fusion so as to reduce the number of transmitted information to the sink. The clusters formation is based on the energy reserve of sensor nodes and its proximity to the cluster head [2]. In hierarchical routing, data moves from a lower clustered layer to higher region, hopping from one node to another which covers larger distances, hence moving the data faster to the sink faster. Clustering provides inherent optimization capability at the cluster heads. A view of the architecture of hierarchical network is as shown in fig 4.

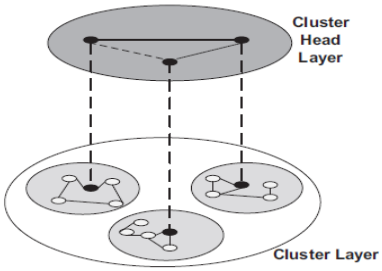

Fig. 4 Hierarchical network architecture.(In hierarchical routing, data moves from a lower clustered layer to higher region, hopping from one node to another which covers larger distances, hence moving the data faster to the sink faster).

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

4. Network flow and QoS-aware protocols

Some of the routing protocols which do not belong to data- centric, hierarchical or location based tend to fit into network flow and QoS-aware approach. In some protocols, routing setup is modelled and treated as a network flow problem, while in QoS-aware protocols, end-to-end delay is the major metric considered when setting up paths or routing in the sensor network.

C. Proactive routing protocols: proactive protocols compute all the routes before they are actually needed, and the routes are stored in a table format called a routing table in each node. Each node stores information on routes to every other node in the network. The settling time for a network using this kind of algorithm is extremely high, and the number of messages exchanged in order to maintain route in formation does grow at an alarming rate, hence, limiting the scalability of the algorithm.

D. Reactive routing protocols: reactive protocols compute routes only when they are needed. In this class, each node store routes only to its immediate neighbours, and determine multi- hop routes as required. In reactive protocols, routing table maintenance overhead is drastically reduced in lieu of the time required to send a message, as the path has to be determined each time a packet has to be transmitted across multiple hops to the sink.

E. Hybrid routing protocols: hybrid protocols use the combination of reactive and proactive strength, and use a proactive system within a given radius, while using reactive system in determination of routes to nodes outside the radius. The radius is always a function of some metric like the number of hops.

F. Energy efficiency: it is a measure of the ratio of total packet delivered at the sink node (base station) to the total energy consumed by the network's sensor nodes(k bits/s).In most cases, sensor nodes a reequipped with small and non-rechargeable batteries, usually of few ampere-hours. Therefore, the efficient battery energy utilization of a sensor node is a critical aspect to support the extended operational lifetime of the individual nodes and of the whole network. A WSN routing protocol is expected to:

(i) Minimize the total number of transmissions involved in route discovery and data delivery, and

(ii) Distribute the forwarding of the data packets across multiple paths, so that all nodes can deplete their batteries at a comparable rate.

VI. EN-ROUTE FILTERING SCHEMES

In WSN internal attacks are not detectable by cryptographic techniques. The unattended operation makes it easy to compromise the sensor node and to release the information to the adversary .Adversary can launch internal attack that cannot be solved by cryptographic technique. Such internal attacks can be solved by en-route filtering scheme. En-route filtering means that not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops the bogus message travels and, thereby, conserve energy. Hence, it is especially useful in mitigating false data injection attack and path based DOS attack because the falsified messages will be filtered out as soon as possible.

A. Statistical en-route filtering (SEF): Statistical en-route filtering (SEF) [13] is the first en-route filtering scheme proposed by F. Ye, H. Luo to address the fabricated report injection attacks in the presence of compromised nodes and introduce an en-route filtering framework. Each event detecting sensor endorses the report by producing a keyed MAC using one of its stored keys.. A report with insufficient number of MACs will not be forwarded. When the sink receives event reports, it can verify all the MACs carried in the report because it has complete knowledge of the global key pool. False reports with incorrect MACs that pass through en-route filtering will then be detected. The SEF mechanism (Statistical En-Route Filtering) detects and drops bogus reports from compromised nodes. The verifying of MACs is done probabilistically. SEF can't detect which nodes are compromised because reports are filtered en-route probabilistically, but it can prevent the false data injection attack with 80 - 90 percent probability within 10 hops. Otherwise this method is not very efficient.

B. An interleaved hop-by-hop authentication scheme (IHA): Zhu et al. proposed an interleaved hop-by-hop authentication (IHA) scheme [26]. In this scheme, the base station periodically initiates an association process enabling each node to establish pair wise keys with other nodes that are n hops away, which is a security threshold. All nodes are detecting nodes and forwarding nodes, generating reports about events, forwarding them, and verifying report correctness. At least t+1 node must agree on a report for it to be considered valid. IHA requires the existence of a fixed path for transmitting control messages between the base station and every cluster-head. The high communication overhead incurred by the association process makes IHA unsuitable for the networks whose topologies change frequently.

C. Commutative cipher based en-route filtering (CCEF): Yang et al. presented a commutative cipher based en-route filtering (CCEF) scheme [17]. In CCEF, each node is preloaded with a distinct authentication key. When a report is needed, the base station sends a session key to the cluster-head and a witness key to every forwarding node along the path from itself to the cluster-head. The report is appended with multiple MACs generated by sensing nodes and the

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

cluster-head. When the report is delivered to the base station along the same path, each forwarding node can verify the cluster-head's MAC using the witness key. The MACs generated by sensing nodes can be verified by the base station only. CCEF has several drawbacks. First, it relies on fixed paths as IHA does. Second, it needs expensive public-key operations to implement commutative ciphers. Third, it can only filter the false reports generated by a malicious node without the session key instead of those generated by a compromised cluster-head or other sensing nodes.

D. Location-based resilient security (LBRS)

Yang et al. proposed a location-based resilient security (LBRS) scheme [18]. In LBRS, a sensing field is divided into square cells, and each cell is associated with some cell keys that are determined based on the cells location. Each node stores two types of cell keys. One type contains the keys bounded to their sensing cells to authenticate the reports from those cells. The other type contains the keys of some randomly chosen remote cells, which are very likely to forward their reports through the nodes residing cell. The authors introduced several types of report disruption attacks in which adversaries can intentionally attach invalid MACs to legitimate reports to make them dropped by other nodes. However, they did not provide a concrete solution. In addition, LBRS suffers a severe drawback: It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. However, to the best of our knowledge, most of the practical sensor localization approaches [32] cannot be finished in such a short time slot, and even the localization process itself is vulnerable to various attacks

E. Dynamic en-route filtering (DEF) scheme: In the Dynamic En-route Filtering (DEF) scheme by Yu and Guan [32] [16], a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. Before deployment, each node is preloaded with a seed authentication key and secret keys randomly chosen from a global key pool. Before sending reports, the cluster head disseminates the authentication keys to forwarding nodes encrypted with secret keys that will be used for endorsing. The forwarding nodes store the keys if they can decrypt them successfully. Each forwarding node validates the authenticity of the reports and drops the false ones. Later, cluster heads send authentication keys to validate the reports. The DEF [30] scheme involves the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited sensors.

F. Secure ticket-based en-route filtering: Secure Ticket-Based En-route Filtering (STEF) [6], proposed by Krauss et al., uses a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. If a packet does not contain a valid ticket, it is immediately filtered out. STEF is similar in nature to SEF and DEF. The packets contain a MAC and cluster heads share keys with their immediate source sensor nodes in their vicinity and with the sink. The downside of STEF is its one way communication in the downstream for the ticket traversal to the cluster head.

VII. CONCLUSIONS

This paper presents the some security and routing relevant issues of WSN.A literature review about the security requirements, various possible attacks on WSN are described. In this paper we study about the design and routing factors needed for Wireless sensor networks. Finally an analysis about the routing protocols. To address such problems in the presence of compromised sensor nodes en-route filtering schemes are essential. Also an analysis about these en-route filtering scheme is made in this paper. A case study is provided as a guidance to select the suitable routing protocol.

Currently, there is very little research that looks at handling QoS requirements in a very energy constrained environment like sensor networks. Also, routing protocols should node mobility. Most of the current protocols assume that the sensor nodes and the sink are stationary. However, there might be situations such as battle environments where the sink and possibly the sensors need to be mobile.

We hope that this will encourage protocol designers to take into account the various protocol characteristics when designing an efficient protocol; QoS awareness, energy efficiency, mathematical models, simulation environment and settings, and finally real time implementation. This will then enable and facilitate more research on the set goals as well as allow researchers to perform fair comparison.

REFERENCES

[1] Ferreira, A. C., Vilaca, M. A., Oliveira, L. B., Habib, E., Wong, H. C., and Loureiro, A. A. F., "On the security of cluster based communication protocols for wireless sensor networks", In 4th IEEE International Conference on Networking (ICN'05), volume 3420 of Lecture Notes in Computer Science, pp. 449–458, Reunion Island, April 2005.

[2] Akkaya, K., Younis MA., "Survey on routing protocols for wireless sensor networks", Ad Hoc Networks, 3(3), pp.325–49, 2005.

[3] Kumar, A., Saxena, N., Tsudik, G., and Uzun, E., "Caveat Emptor: A Comparative Study of Secure Device Pairing Methods", Proc. Int'l Conf. Pervasive Computing and Comm. (PerCom '09), 2009.

[4] Akyildiz IF., Su W., Sankarasubramaniam Y., Cayirci E., "Wireless sensor networks: a survey", Computer Networks, 38(4), pp.393–422, 2002.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

[5] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., and Culler, D.E., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5., pp. 521-534, 2002.
[6] Kraub, C., Schneider, M., Bayarou, K., and Eckert, C., "STEF: A Secure Ticket-Based En-Route Filtering Scheme for Wireless Sensor Networks", Proc. Second International Conf. Availability, Reliability and Security (ARES 07), pp. 310-317, Apr. 2007.
[7] Celik, F., Zengin., Tuncel, S. A., "Survey on swarm intelligence based routing protocols in wireless sensor networks", International Journal of the Physical Sciences, 5(14), pp.2118–26, 2010.
[8] Chong, C-Y., Kumar, SP.,"Sensor networks: evolution, opportunities, and challenges", Proceedings of the IEEE, 91(8), 1247–56, 2003.
[9] Daojing He., Lin cui., Hejiao Hang., "Design and verification of Enhanced secure localization scheme in wireless sensor network ", IEEE Transaction On parallel and distributed systems vol. 20 no.7 ,July 2009.
[10] Balfanz, D., Smetters, D.K., Stewart, P., and Wong, H.C., "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks", Proc. Symp. Network and Distributed Systems Security, 2002.
[11] Liu, D., and Ning, P., "Establishing Pairwise Keys in Distributed Sensor Networks", Proc. ACM Conf. Computer and Comm. Security (CCS '03), 2003.
[12] Dorigo, M., "Solve difficult optimization problems: Lecture notes in computer science", In: Proceedings of the 6th European conference on advances in artificial life table of contents, vol. 2159, pp. 11–22, 2001.
[13] Ye, F., Luo, H., Lu, S., and Zhang, L., "Statistical en-route detection and filtering of injected false data in sensor networks", in Proc. IEEE INFOCOM, vol. 4, pp. 2446–2457,2004.
[14] Handy, MJ., Haase, M., Timmermann, D., "Low energy adaptive clustering hierarchy with deterministic cluster-head selection", In: Proc. of the 4th IEEE Conf. on Mobile and Wireless Communications Networks, Stockholm: IEEE Communications Society, pp.368-372, 2002.
[15] Chan, H., Perrig, A., and Song, D., "Random Key Predistribution Schemes for Sensor Networks", Proc. IEEE Symp. Security and Privacy, 2003.
[16] Hou, H., Corbett, C., Li, Y., and Beyah, R., "Dynamic Energy- Base Encoding and Filtering in Sensor Networks", Proc. IEEE Military Comm. Conf. (MILCOM 07), Oct. 2007.
[17] Yang, H., and Lu, S., "Commutative cipher based en-route filtering in wireless sensor networks", in Proc. IEEE VTC, vol. 2, pp.1223–1227, 2004.
[18] Yang, H., Ye, F., Yuan, Y., Lu, S., and Arbaugh, W., "Toward resilient security in wireless sensor networks", in Proc. ACM MobiHoc , pp. 34–45, 2005 .
[19] Karaki, JN., Kamal, AE., "Routing techniques in wireless sensor networks: a survey", Wireless Communications, 11(6), pp.6–28, IEEE 2004.
[20] Karlof, N., Sastry..,and Wagner, D., "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proc. Second Int'l Conf. Embedded Networked Sensor Systems, 2004.
[21] Krishnamachari, B., Estrin, D., Wicker, S., "Modeling data-centric routing in wireless sensor networks", In: Proceedings of the IEEE INFOCOM, New York, 2002.
[22] Eschenauer, L., and Gligor, V.D., "A Key-Management Scheme for Distributed Sensor Networks", Proc. ACM Conf. Computer and Comm. Security (CCS '02), 2002.
[23] Bandyopadhyay, S., and Coyle, E. J., "An Energy Efficient Hierarchical Clustering Algo-rithm for Wireless Sensor Networks", in Proceeding of IEEE INFOCOM'03, San Francisco, April 2003.
[24] Singh, SK., Singh, MP., Singh, DK., "Routing protocols in wireless sensor networks-a survey", International Journal of Computer Science and Engineering Survey (IJCSES);1(2) ,pp.63–83,2010.
[25] Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, GJ., "Protocols for self-organization of a wireless sensor network", IEEE Personal Communications, 7(5), pp.16–27, 2000.
[26] Zhu, S., Setia, S., Jajodia, S., and Ning, P., "An interleaved hop-by-Hop authentication scheme for filtering of injected false data in sensor networks", in Proc. IEEE Symp. Security Privacy, pp. 259–271, 2004.
[27] Du, W., Deng, J., Han, Y.S., and Varshney, P.K., "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks", Proc. ACM Conf. Computer and Comm. Security (CCS '03), 2003.
[28] Yang, Z., Mohammed, A., "A survey on routing protocols for wireless sensor networks", Ad Hoc Networks, 3, pp.325–49, 2005.
[29] Wang, Y., Attebury, G., Ramamurthy, B., "A survey of security issues in wireless sensor networks", IEEE Communications Surveys & Tutorials 8 (2), pp. 2–23, 2006.
[30] Zaman, N., Abdullah, AB., "Energy efficient routing in wireless sensor network: research issues and challenges", In: Proceedings of IEEE international conference on intelligence and information technology, 2010.
[31] Zhang, Y., Kuhn, LD., Fromherz, MPJ., "Improvements on ant routing for sensor networks, Ant colony optimization and swarm intelligence", Lecture notes computer science, pp. 289–313, 2004.
[32] Zhen Yu., and Yong Guan., "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks ", IEEE/ACM Transactions On Networking, Vol. 18, No. 1, February 2010.

ACKNOWLEDGMENT

We take this opportunity to express our deepest gratitude and appreciation to all those who have helped us directly or indirectly towards the successful completion of this paper.

BIOGRAPHY

Mr.D.Gopinath received his B.Sc and M.Sc degree in Computer Science from the Bharathiar University. He is currently Research Scholar in Kongu Arts and Science College. He had presented papers at National and international conferences. His research interest include Wireless sensor Network Security, Network Security, especially design and implementation of security metrics

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

Mr.P.Ramesh, Head, Department of Computer Science in Kongu Arts and Science College, Erode. He received the B.Sc Degree under Bharathiar University, M.Sc Degree under Bharathidasan University and M.Phil under Manonmanium Sundaranar University – Tirunelvelli. Currently he is doing his Ph.D under Bharathiar University. He had presented more than 20 papers in National and international conference.