Security Analysis of Wireless Sensor Network
A Literature Review

Mohammad Hossain, Umme Muslima, Humayra Islam,
Lecturer, Electronics & Electrical Engineering Department,
University of Information, Technology & Sciences (UITS),
Baridhara, Dhaka – 1212, Bangladesh.
mohammadandhossain@gmail.com

***Abstract*— Security was a prior concern to the researchers since the beginning of wireless sensor network. With the growing technology, the belongings on security are also advancing day by day. Though it was tried to formulate this network completely secured during the time of designing, intruders and attackers always find their way to get inside it and accomplish their disgraceful intention. Different research papers have shown different ways to keep the network secured and trustworthy. This paper presents a significant analysis on the security issues of wireless sensor network. Literature study on various articles are accumulated where both possible security violence and their solutions are focused from most recent research papers which will be very helpful for future work for the researchers. Moreover, some basic implications are also proposed to keep the network away from vulnerability and interception.**

Keywords—Sensor; Security; Vulnerability; Interception; Trustworthy

I. INTRODUCTION

In any kind of wireless networks security and confidentiality are essential issues. In wireless sensor network (WSN) the importance of security is more challenging. Wireless sensor network (WSN) and its applications are attacked by Intrusions and other attacks to interrupt the characteristics it serves. Wireless sensor network is usually provided to the remote areas. Wireless sensor network is used to determine the different environmental monitoring applications such as temperature, air pressure, humidity finding [16]. Since sensor networks are frequently used in remote areas and in those areas, the operation of the network is left unattended, and unmonitored regularly that help the intruders to make an easy target for substantial attacks, unconstitutional access and tempering. Sensor nodes have to compromise with attacks due to resource tapered activities and operating in insensible surroundings also difficult to differentiate security violations from node failures. Problems are also created in justifying link qualities and overall shut down of the network. These resource limitations need security mechanisms that are designed for WSN applications, so that the limited resources can be used proficiently. This paper presents the different verities of common attacks which are threatening this network since the beginning of its operation. Then recent trend in security mechanism improvement has been shown briefly. Most of the security solutions are studied from recently published international journals and conference papers which will be very helpful for future researchers to work onward.

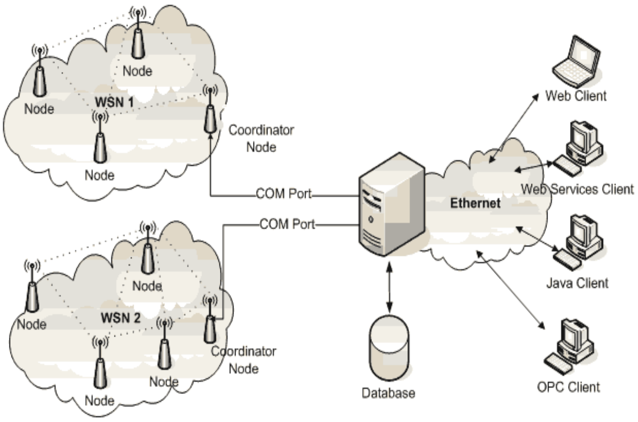

Fig. 1. A simple wireless sensor network [1]

II. SECURITY FUNDAMENTAL OF WSN NETWORK

To keep the wireless network secured, we have to protect it from unauthorized access or unintended uses. There are three important services for the security mechanisms are Confidentiality, Integrity and Availability are defined by The CIA security model [2]. Confidentiality defines that any unlawful access to the network must be prohibited. Only reliable node of the network can access the resources. Integrity describes that a message must reach from sender to receiver without changing or modification. Sensitive information must not be accessed or changed by unauthorized individual.

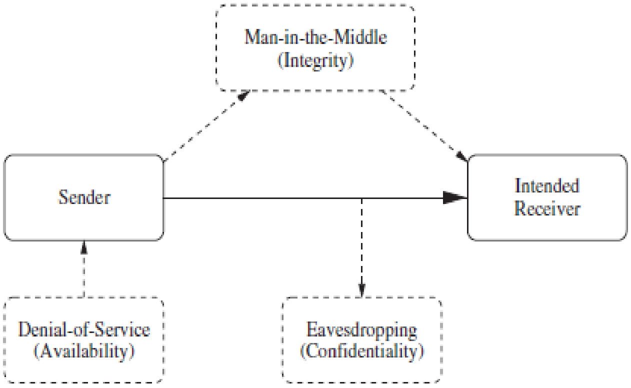

Fig. 2. Different types of attacks in the CIA model [2]

Availability ensures all time uninterrupted access to the network for the legitimate nodes. Figure 2 shows some common attacks present in CIA model. To prevent the reception of a message by an unauthorized individual which is called Eavesdropping, appropriate confidentiality procedure can be followed. A man-in-the-middle attack is when an unauthorized bad guy receives a message from the sender then alters it before sending to the receiver. The innocent receiver never knows whether the message came from and what happened on transmission. And, a denial-of-service attack describes to an intruders effort to interrupt the transmission or service that a sender provides to its receiver. Beyond these three attacks of CIA model, authentication is another mentionable term of establishing or confirming the identity of a user or a station, verifying that a data arrived from who it declares to have come from. Digital signature supports both authentication and acknowledgement of receiving the data to the appropriate receiver. Each communication network has its own way of integrity, confidentiality and availability. Security of network also relates with cryptography which are also divided in some other sections. In symmetric key cryptography, the encryption and decryption of a message between two communication parties use a single key sharing algorithm method. The encryption-decryption techniques applied for the conventional wired networks are not suitable to be applied directly for wireless sensor networks [17].

III. SOME COMMON ATTACKS IN WSN

Wireless networks are susceptible to security attacks because of the broadcast nature of the transmission medium. Furthermore, as WSNs nodes are unfriendly unsafe which are physically unprotected because of location which adds an extra vulnerability to security. It's really difficult and complicated to supervise each node and defend them, when a sensor network is really outsized. Different types of security threats are always formed by the attackers to formulate the WSN system unsteady and unstable. Here different types of WSN security threats are stated to obtain a general idea on the security system of this network.

A. Outsider and Insider Attacks

The attacks which arise by outside stations [3], [4] are defined as outside attacks. Insider attacks arise when genuine nodes of a WSN perform in unintended or unauthorized customs. Robustness against outsider is important to overcome this problem [3]. Realistic Levels of Security must ensure to overcome the insiders from inside attack of network.

B. Passive versus Active Attacks

Wireless sensor network is constructed with hundreds of thousands of sensor nodes with one or more base stations by which all the functions of transmission are done for the sensor node stations [55]. Eavesdropping or monitoring of data exchanged during transmission is passive attack. But active attack includes direct changing the information or modification of packets during transmission.

C. Interruption

The main purpose of this kind of attack is to bring out denial-of-service (DoS) attack. Sometimes the transmission link becomes disconnected or lost. The service availability faces threatens and gets interrupted. Any layer in the network model may face challenge by the attackers and be interrupted. The challenger can compromise the users/nodes of sensor network to deal with it. But, it does not have the capability to cheat all the nodes at the same time [20].

D. Interception

When attacker gains unauthorized access to sensor node or data in it sensor network is compromised by an opponent. is an example of this scenario is node capture attack. Privacy of message in application layer is threatened due to this. An adversary may add some extra information to the authorized packet and make it enlarge which would be difficult for the legitimate receiver to work out. Sometimes the extra unnecessary data attached later on are so massive that the original contents loose its priority and thus intercepting the whole information [22]. Any subscriber station (SS) must get proper authentication before getting access to the network [24].

E. Modification

Reliability of message diminishes when attackers modify or alter the information in a message and confuse or deceive the receivers completely. Modification is major threat at network and application layer. An encryption channel communication settings may help to obtain data privacy. A unique initialization vector for each encryption scheme to make variation to the cipher text can confirm semantic security as a probabilistic encryption scheme [23].

F. Fabrication

Message authenticity is threatened when trustworthiness of information is compromised and an adversary injects false data to the information message. The key motive is to confuse or deceive the stations connected in the communication scheme. By overflowing the network, DoS can also be attacked.

G. Host Based Attacks

There are three types of host based attacks [6]. These are user compromising, hardware compromising, software compromising. In user compromising process, the user nodes in WSN are managed to provide faithful information to the intruders such as passwords, keys of the sensor nodes. In hardware compromising extraction of the program code, data, keys stored in sensor nodes are revealed by a process call tempering. Software compromising includes breaking down the software code that runs to sensor nodes. Buffer overflows takes place when the operating system or the application running into the sensor nodes are susceptible.

H. Network Based Attacks

The two main types of network base attacks are layer based attack and protocol based attack [6]. These attacks mostly work on information during transmission time. These attacks also depart from the protocol. Besides of service availability, message confidentiality, integrity and authenticity of the network, an insider of the network achieves unreasonable benefit for itself in the usage of the network. The attacker does self-centered conducts which disrupts the dedicated functioning of the protocol.

I. Jamming

This is kind of Denial of Service attack. An adversary attempts to disturb the working procedure of the network by covering high powerful signal. Attacking in WSN nodes classified [7] as constant disrupt, deceptive and reactive functions. The packets are corrupted in regular time interval due to constant disruption. Deceptive function occurs when the attacker disguises himself as a justifiable node and sends constant bit stream. Also when an attacker senses traffic and sends a jam signal. Spread spectrum technique in radio communication system helps to avoid these types of attacks.

J. Radio Interference

Radio interference is called where the opponent either produces large amounts of obstacle intermittently or tirelessly. Symmetric key algorithm is been used in which revelation of the keys delayed by some time intermission to avoid this problem [3].

K. Tempering or Destruction

It is possible for him to find out sensitive information like as cryptographic keys or other important information when an attacker gets physical access to a sensor node. Self-devastation or tamper-proofing package is one solution of this [4]. In this process, when an outsider touches a sensor node physically, the node itself removes all its data or information and saves its own from the attacker. Whenever someone unauthorized or unconstitutional tries to access the node, it vaporizes the evidence and turn into empty.

L. Continuous Channel Access

When a malicious node constantly sends packet over the channel, it disrupts the access of other authentic nodes by keeping busy the media access control protocol. One resolution to this type of attack is that MAC admission control can pay no consideration to extreme requests from a particular node when it does so. Time division multiplexing method can be another option. Each station will be accessing the network in a suitable manner [8], [4].

M. Collision

Collision occurs when two nodes try to send packet on the same time and same frequency. Packets loss, errors originate in checksum at the receiver and therefore the receiver discarded the message. An outsider tries to do match with a legitimate node to send data exactly with it to keep the genuine node down from the network. To overcome this problem, error correcting code is used [8], [4].

N. Unfairness

An illegal use of MAC layer mechanism hinders its regular activities call unfairness when collision or continuous accessing of channel takes place on MAC layer. This has a bit similarity with DoS attack but ended with minor act scarcity. Usage of small frames by any individual node is must. It is needed so that any node gets the channel only for a small time period is good methodology to this type of susceptibility [8], [4].

O. Sybil Attack

In Link Layer this is a common attack. A malevolent node illegitimately takes on multiple individualities. An opposition can present in more than one place as a single node and presents several identities to other nodes in the network. This can extensively decrease the effectiveness of fault tolerant schemes distributed storage, dispersity [13] and multipath [14]. It may be really complex for an opponent to inaugurate such an attack in a network where each pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Figure 3 shows a typical Sybil attack.

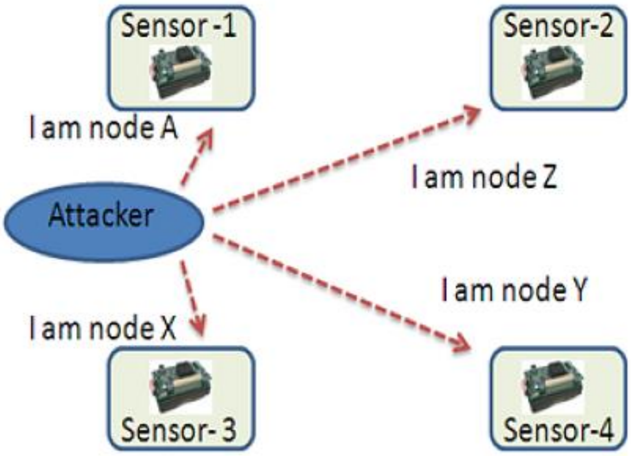

Fig. 3. Sybil Attack [15]

P. Sink Hole Attack

In this attack a node present in the WSN network is conceded to the nearby nodes with respect to the routing algorithm. Neighboring nodes are attracted to the conceded node. A metaphorical sinkhole is created with opponent staying at the centre. Routing protocols named geo-routing protocol is defiant to sinkhole attacks. Geo-routing protocol uses the topology which is assembled using only localized information and traffic is naturally routed through the physical location of the sink node. This formulates it hard to tempt it somewhere else to make a sinkhole. [10], [4], [5] and [11].

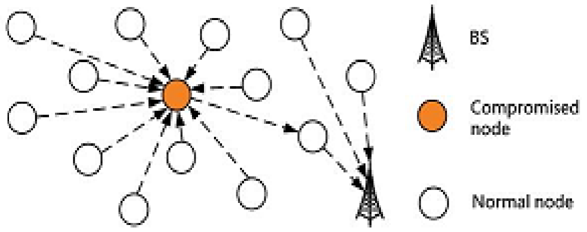

Fig. 4. Sinkhole Attack [56]

Q. *Hello Flood*

In this attack an intruder sends HELLO packets to neighboring nodes informing them the survival of its own so that it can obtain and send them information packets. Laptop-class adversaries interconnect with such kind of packet to nodes in a particular area and make them believe that a genuine node is accessing with them. A large number of nodes within the network thus start sending packets to this invented node and mistreated. Proper authentication is the solution to this types attack. The information arrived to a node must be bi-directionally checked to avoid such trespassers to get inside into the network as a legitimate one to cheat [10], [4], [5], [11].

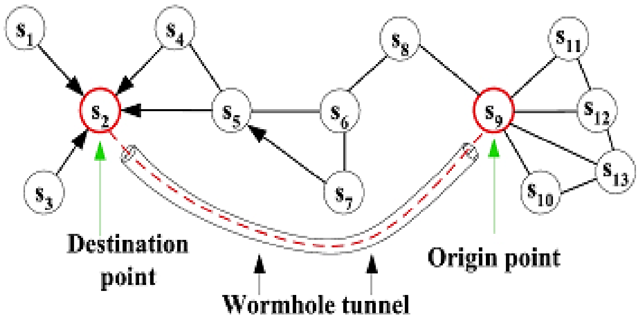

Fig. 5. Wormhole Attack [56]

R. *Wormhole Attacks*

An adversary passageway messages received in one part of the network over a low latency construction and replays them in a different part of the network in this attack. An adversary completely disrupts routing who is closely situated with the base station by creating a well-placed wormhole. Some nodes that are generally are multiple hops distant from a base station influenced by the adversary who are only one or two hopes away from them. They also find an easy way to transmit messages to the base station. Because of short distance and high quality the new route is attractive to the legitimate nodes. This problem can overcome by making the original topographical route shortest from nodes to base station. Also it can be done by using very small period of time to coordinate among the nodes [8], [4] and [5].

IV. INSECURITY PROBLEM

The rate of malicious work increases when security is compromised. Data communication is interrupted in a compromised network. It cannot be confirmed that all data packets must reach from sender to receiver in an unsecured network. When the security decrease gradually, transmitted packets may also drop and even the transmission rate can become zero. Figure 6 and 7 have shown that how packets dropped are increases when malicious ratio increases and how delivery of packets decreases when malicious ratio increases gradually [12].

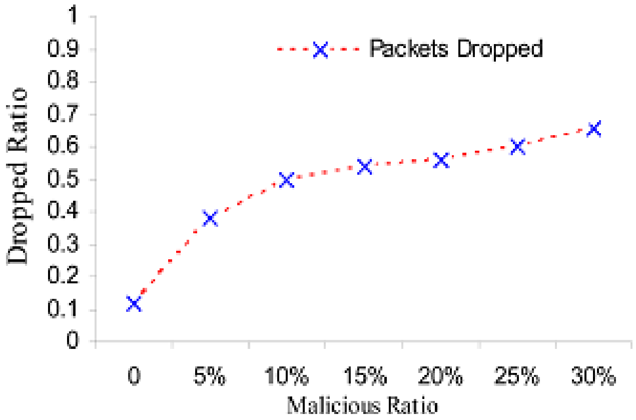

Fig. 6. Malicious ratio significantly increases athe amount of packets dropped.

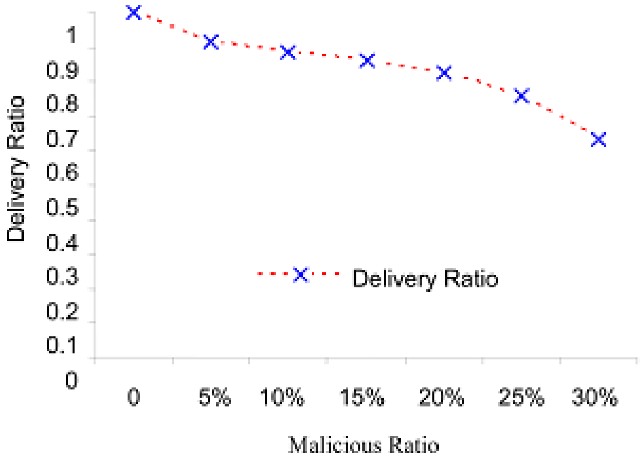

Fig. 7. Malicious ratio decreases the delivery ratio of packets.

Each and every small node in a network must be secured in order to maintain the full security in WSN [19]. To mitigate confidentiality and authentication a secure triple key management scheme (STKS) can be used [18].

In order to obtain the full security in WSN, implementation of security mechanism must be confirmed to all small nodes of the big network [19]. Future security mechanism should focus on characteristics of nodes and related communication protocol. The design and completion must also reflect on consuming less power by wireless sensor network. The μTesla protocol proposed by Perrig to present secure broadcast authentication considering free time synchronization between sensor nodes [3]. The time management does not need for one way hash chain algorithm because it is used to clarify the request result itself, not the substance of demand significance [21].

V. RECENT SECURITY SOLUTIONS

A. *Re-Keying Method*

"Reference [25]" has proposed this approach, where re-keying is initiated by the sensor node only if any two consecutive keys are invalidated. Two parameters r_i and r_{i+1} have to be pre-set once all the sensor nodes are ready to deploy in the field. To communicate with the Base Station, a new re-keying key will be produced by one hash function. The key assortment technique uses the node ID and some basic rotate and multiplication functions present to select the key for current data transmission. Because of this dynamic key selection, this approach recognizes the replay attack, DoS attack and Sybil attack.

B. *Telosb Mutual Authentication*

"Reference [26]" proposed a mutual authentication protocol between sensor nodes and gateway nodes. It has shown that multiple security techniques against different security threats, such as time stamps against replay attacks, the ZUC encryption algorithm against data eavesdropping and unauthorized falsification. To verify the effectiveness and efficiency of that scheme, Telosb based wireless sensor test bed is implemented. A light weight dynamic mutual authentication protocol using one way hash function and random nonce are realized on the Telosb based platform.

C. *Energy Efficient Key Management Scheme*

"Reference [27]" proposed an algorithm that supports the formation of three types of keys for each sensor node, an individual key shared with the base station, a pair wise key shared with neighbor sensor node, and finally a group key that is shared by all the nodes in the network. The algorithm used for establishing and updating these keys which are energy efficient and lessens the involvement of the base station. To calculate the keys during initialization, membership change and key compromise polynomial function is used. From time to time the key will be updated. To overcome the problem of energy inadequacy and memory storage and to provide adequate security, the energy efficient scheme is proposed. It works well in undefined deployment environment. Unapproved nodes should not be allowed to establish communication with network nodes. This scheme when compared with other existing schemes has a very low overhead in reckoning, communication and storage.

D. *Jammed Region Mapping Technique*

"Reference [28]" proposed faster mapping of the jammed regions which is a light-weight technique. It reduces the load on the sensors by removing the actual responsibility of mapping from the network to the central base station (BS). After a few nodes report to the BS, it carries out the task of mapping of the jammed regions in the network. It projected an efficient mapping protocol which relieves the sensor nodes from sending many mapping messages. The mapping results can be improved by having more nodes send jamming notification messages to base station, which creates a trade off between performances of mapping versus the network overhead. The paper also validates that this system requires less interaction among the sensor nodes associated with previous work and thus has less overhead and faster mapping.

E. *Sybil Attack Detection*

False data can be sending to the neighbors when a Sybil node acts as a sender. When it acts as receiver, it can receive the data which is originally intended for a legitimate node. "Reference [29]" proposed a solution which is based on sending and responding to the query sent by the cluster head. The Cluster head has a list of its sub nodes parameters. The parameters are the identities of their location. The Cluster head broadcasts a query packet to all the sub nodes in such a way that it expects a reply that all the sub nodes must send their identity and location. The Sybil node reacts for three cases. When all the genuine sub nodes including Sybil node receive a query packet, it does not respond to it, it simply gets the packet and drops it. The Sybil node does not respond whenever retransmission is done for multiple times. In this case, all the authentic sub nodes respond to the cluster head with their individuality and position. The Sybil node also responds to the cluster head with any one of the Sub nodes identity and its own location. For example, If a cluster head has 4 nodes say 1,2,3,4 with the location x, y, z, a respectively, Sybil node must have any one of these identity (1/2/3/4) and its own location d. The cluster head already has the set of legitimate nodes identity and location. Conflicts ascend when the legitimate node and Sybil node has same and different location. The node with the different location is detected as Sybil node.

F. *Privacy Providing Using Mobile Sinks*

In routing the data from source to sink, various types of active and passive attacks are possible. "Reference [30]" projected new technique to prevent these attacks. The mobile sink is been deployed in the network whose responsibility is to collect data from the sensor node at the same time deliver data to fixed base station. In the proposed technique, the data privacy is ensured in the mobile sink. In Wireless Sensor Network sink inserts the query into the Network, as a result sensor nodes respond to the query and the traffic depends on number of queries engendered per mean time. If sensor nodes have information about query then it responses to sink, otherwise it floods the query to the other nodes.

Through some routing protocol the sensor node will reply to the sink node. In such situation various type of active and passive attacks are possible. In this proposed technique mobile sinks have been deployed to prevent attacks in the network which is responsible for gathering and transporting the data to fixed base station.

G. *Priority Based Approach*

"Reference [31]" proposed an approach called "priority based approach (PBA)" and established an association between packet precedence and current energy status of a sensor node which resolves the most urgent message to forward first according to its priority, also its energy level. By giving less priority to the attacker node, it then improves the security of a network. Also, depending upon the energy level and given time to refill the energy, the proposed priority based approach emphasizes reducing the workload on some nodes. Therefore PBA ensures a real time communication in WSN with minimizing the delay and energy spent and maximizing the packet delivery ratio (PDR) and through which further maximization of the lifetime of the network.

H. *Path Based Denial of Service (PDoS)*

"Reference [32]" suggested to defend the path based denial of service (PDoS) attack proposed a novel solution. An attack behavior detection algorithm used triple exponential smoothing and Markov chain. In particular, this algorithm is operated at the base station, which makes the minimum energy consumption of the intermediate nodes. Therefore, they do not need to detect every packet for verifying if they are standard or nonstandard. And two valuation factors are considered, the number of the packets and the energy state of the node. To achieve the accuracy detection these two factors are certain. Meanwhile, it is proposed one hop black holes mechanism in order to completely defend the PDoS attack, , which makes the transitional nodes that are one hop away around the malevolent cluster head (CH) as the black holes. These nodes can just receive the attacked packets which are sent by malicious nodes and drop them.

I. *Secure Toplogy Protocol TLES*

"Reference [33]" proposed a secure topology protocol of WSN, that is, TLES. Trust factors were defined by the node's historical behavior, and the trust value of each node was calculated according to the comprehensive value of direct trust and indirect trust, which are related to the trust factors. TLES uses the idea of clustering. First of all, the cluster heads were selected according to the trust value, residual energy, and density of nodes. Then, the cluster heads choose the next hop node by the residual energy, the distance to BS, and degree of candidate node. After that, the construction of the whole network topology was built. TLES can eliminate the malicious nodes in network effectively, so as to ensure the safety and rationality of node communication.

J. *Authentication Scheme for WSN*

"Reference [34]" deliberated the different authentication techniques appropriate for the severely inhibited sensor nodes in WSNs, and addressed three main categories based on symmetric cryptography, asymmetric cryptography and hybrid techniques using both cryptographic methods. It conversed each category and deduced that RC5 is among the most applicable to use in symmetric key techniques and IBEECC is so far the most promising asymmetric key cipher. The choice of which category to use, depends on the environment of the network, the attacker model and the sensitivity of the data being sensed. It is considered the findings in a centralized trust-based routing protocol for WSNs called CENTER and based on the different needs and criteria showed how to choose the most appropriate authentication technique for higher security and verification of WSN.

K. *Secure Localization and Location Verfication of WSN*

"Reference [35]" studied localization systems from the security point of view. It presents how an unsafe localization system can be negotiated in a numerous ways to compromise the entire functioning of a WSN this leads to erroneous data aggregation and incorrect decision making. Later on it is proposed the node authentication and key distribution protocol that gives efficient re-authentication method. The protocol requires just three communication passes with one third of communication message sizes compared with existing protocols for the process of node re-authentication. From that of initial node authentication the node re-authentication of a single mobile node achieves about 2–3 times more efficiency for computational overhead.

L. *Virtual Certificate Authority (VCA)*

"Reference [36]" projected an efficient authentication and key exchange pattern for the integrated WSN networks by integrating WSN into mobile networks as the application. This introduces the concept of VCA which is a virtual certificate authority. The issue of initial trust is solved via the structured signing of certificates, which are inserted on devices prior to deployment. Furthermore, VCA also supports node authentication and a private key distribution mechanism. It also enhances many WSN design goals that include simplicity, scalability, interoperability and control for individual manufacturers.

M. *Device Based Asynchronous Ranging and Node Identification for WSN*

"Reference [37]" suggested a distributed scheme for secure ranging and node credentials. The proposed DARNI scheme can be used to detect misbehavior of anti-nodes, to observe the behavior of nodes over time and to decide whether to trust them by applying the device physical characteristics (e.g. internal device delays), the clocking information, and the response delay time. Moreover, associated with a conventional sensor network, incorporating the device physical characteristics allows a wireless sensor network to effectively solve node verification problem without changing any hardware and software infrastructure and reliably provide a secure distance measurement system in wireless sensor networks.

N. *Lightweight Authentication Protocol for WSN*

"Reference [38]" introduced a new and secure protocol based on number theory concepts and correspondent equations to provide authentication between the sensor nodes and Database Server in a Wireless Network. The proposed protocol uses Fermat Number Transform (FNT) and Chinese Remainder Theorem (CRT) to enable secure communication. To reduce the computational complexity involved in existing algorithms, the protocol will be using its own encryption and decryption algorithm. It results in minimum memory utilization, instant authentication and it endures Cloning attack, Replay attack, DoS attack and Man–in–the-middle attack.

O. *LEACH Based Enhanced Protocol for WSN*

"Reference [39]" introduces the SA-LEACH in order to strengthen the security of the cluster-based communication protocol in wireless sensor networks. In the cluster formation phase, certification for candidate cluster head broadcast messages. That is introduced to effectively prevent malicious nodes from becoming cluster head nodes, effectively prevent to join the cluster; introduced the authentication and the identification certification during nodes joining clusters. In the stable phase, to stop attackers from broadcasting counterfeit news to cluster members, introduces the certification mechanism for cluster head broadcast messages of each member node in the clusters.

P. *Countermeasures in Compressive Data Gathering.*

"Reference [40]" identified two statistical assumption attacks against compressive data gathering and shows that traditional approaches may suffer serious information leakage under these attacks. Particularly, the estimation error of compressive data gathering was analyzed quantitatively through extensive statistical analysis, based on which it proposed a new compressive data aggregation scheme by adaptively changing the measurement coefficients at each sensor and correspondingly at the sink without the need of time synchronization. In this analysis, it is shown that the proposed scheme could significantly improve the data confidentiality at a light computational and communication overhead.

Q. *Sensor Authentication in Collaborating Sensor Network.*

"Reference [41]" addressed a new security problem in the dominion of collaborating sensor networks. Collaborating sensor networks, refers to the networks of sensor which collaborating on a mission, each sensor network is independently owned and operated by separate entities. These independent networks are practical where a number of independent entities can deploy their own sensor networks in multi-national, commercial, and environmental scenarios, and some of these networks will integrate complementary functionalities for a mission. In the scenario, it addressed an authentication problem where in the goal is for the Operator o^i of Sensor Network s^i to correctly determine the number of active sensors in Network s^i. Such a problem is challenging in collaborating sensor networks where other sensor networks, despite showing intent to collaborate, may not be completely trustworthy and could compromise the authentication process. The research proposed two authentication protocols to address this problem. These protocols rely on Physically Unsolvable Functions, which are a hardware based verification primitive exploiting inherent randomness in circuit fabrication. These protocols are light-weight, energy efficient, and highly secure against a number of attacks.

R. *Hybrid Key Management for Heterogeneous WSN*

"Reference [42]" presents an efficient hybrid key management method based on heterogeneous networks. In this method, a secure link through signature encryption algorithm for communication can be established between cluster heads and base station. Relatively larger energy consumption is needed for this method, but its security is better, and cluster heads and the base station have enough energy to understand the algorithm. To establish a shared symmetric key which is used for communicating between cluster head and nodes in its cluster the ECDH key exchange algorithm has been adopted. Energy limited nodes in the cluster adopts one-way hash function to establish a session key and it is effective in reducing the energy consumption within the cluster nodes on the basis of safety. According to the different situations the key updating adopts different methods to save energies. The proposed method can provide better security, scalability, connectivity and it can save storage space.

S. *Key Management Technique for WSN*

"Reference [43]" proposed a combination of symmetric and asymmetric key primitives at different levels of hierarchy which has been applied to minimize the energy overhead. When security protocols are applied to resource constrained sensor nodes, most of the energy is consumed in communication and computational operations. The resource consuming IBK technique is applied between cluster heads and the base station only to minimize these overheads and at the same time to provide the required security level. The proposed key management technique proves to be better than the probabilistic key pre-distribution and the IBK techniques, when applied separately in the nodes. The secured cluster formation and key reinforcement mechanisms are applied in this scheme to restrict the node capture attack and other network attacks to the cluster alone.

T. *Efficient Public Key Infrastructure for WSN*

“Reference [44]” proposed own public key infrastructure (PKI) for WSN. Main trade-off of this PKI is the high cost of high end sensor nodes (H-nodes). However, it is rational that this method needs much smaller number of H-nodes than low end sensor nodes (L-nodes). Public key cryptography (PKC) not only solves this problem elegantly, but also provides enhanced security services such as non-repudiation and digital signatures. If we want to take the advantage of PKC, each node must have a public key of the corresponding node via an authenticated process. The most broadly used way is to use digital signatures signed by a certificate authority which is a part of a public key infrastructure (PKI). Since conventional PKI requires a huge amount of computations and communications, it can be heavy burden to WSN. Using heterogeneous sensor networks (HSN) with elliptic curve cryptography (ECC), and (k, n) threshold scheme, the PKI becomes energy efficient and scalable while it is flexible to a node capture attack.

U. *IPv6 Enabled WSN*

“Reference [45]” presented an intrusion detection system that can be used as a complement to other available security mechanisms to detect and to report security attacks. Instead of limiting this proposed system to a pre-defined and unambiguous type of attack, it tries to model possible activities of incorrect behavior in a particular region of a WSN. This paper proposed a network-based approach to detect the intrusion in IPv6-enabled wireless sensor networks. It takes the commodities advantage of a well-known protocol suite like the IP stack (e.g., UDP commands). Then, it was possible to create a standards-compliant system that can be deployed in a variety of different WSNs, so long as they maintain the IP stack to an assured degree. Moreover, a *test bed* was created to authenticate the proposed intrusion detection system.

V. *Sequential Hypothesis Testing in WSN*

“Reference [46]” presents a method to detect Sybil attacks using Sequential Hypothesis Testing. The proposed method has been tested using a Greedy Perimeter Stateless Routing (GPSR) protocol with analysis and simulation. The simulation results demonstrate that the proposed method is vigorous against detecting Sybil attacks. The projected method works with general observations carried by each and every node in the network. In addition, the presented method detects the Sybil attacks precisely without having false impact of false positives and false negatives. Distributed nature of the proposed methods is enabled to go well with the networks, deployed in a large network aspect.

W. *Dynamic Key Management Method for WSN*

“Reference [47]” puts forward a network model of node being captured. The energy in case of dynamic clustering is not only considered, but also it takes the probability of nodes capture into consideration. A kind of dynamic key management method (DKMM) key management method was proposed, and this key supervision strategy allows the more secure node most likely to become the cluster head. Although considering the safety of the cluster head in clustering, the cluster head may still be possible to be caught. So DKMM method considers the possibility of capturing the cluster head. By the consciousness of the cluster head’s re-select and enthusiastically updating of the key mechanisms, it is possible to minimize the risk of information leaking as the cluster head being captured.

X. *Secure Key Renewal and Revocation for WSN*

“Reference [48]” proposed several secure WSN protocols for revocations and regeneration of cryptographic keys in the network based on symmetric encryption and elliptic curve cryptography (ECC). It provides a formal analysis of the security for all given solutions of these protocols using Scythes, an automatic verification tool for cryptographic protocols. All the proposed protocols are proven secure but have different security levels by using different types of keys. Finally it is implemented all the protocols on real testbeds using TelosB motes and compared their efficiency.

Y. *An Intelligent Defense Mechanism for the Security of WSN*

“Reference [49]” proposed an Intruder Detection System (IDS) that uses complicated data fusion technique with neural networks as a decision making tool and a timer as an attack monitor, which incorporates game theoretic modeling for the interaction between an attacker node and a victim sensor node. The collective effect of all these aspects of IDS makes a robust struggle against the packets, attempting to hack the critical information residing in the node. This work combines game theory and artificial neural networks to create defense against intruder attack.

Z. *Detection of Jammer in WSN*

“Reference [50]” proposed a novel approach for revealing of node's unpleasantness level for securing WSN from jamming attacks in cluster-based sensor network. The proposed system uses two modules to detect the maliciousness level. Firstly, it protects the network from those internal nodes that are already announced as jammers. Secondly, it detects those nodes that are becoming an opponent. The result demonstrates that the proposed approach detects the unpleasantness level enormously well and achieves high jammer detection rate and low false detection rate.

VI. SECURITY IMPROVEMENT PROPOSAL FOR WSN NETWORK

Due to the efficient activities in particular areas where regular wireless network is not capable of handling the communication, wireless sensor network efficiently maintain the communication between different users as well as with the nearest base station. The security threatening issue is one of the major drawbacks of this communication system. Malicious or bad intruders are present everywhere and they will remain for ever to gain success of their own by making this types of useful and important network defenseless or imperceptible. Engineers and researchers are also working hard to keep the system trustworthy and highly secured for outsiders. Some important steps should be maintained for uncompromised security of the network is as below.

- Strong cryptographic algorithms should apply for sharing public key – private key management.
- Routing or transmission of packets must be managed with secured and efficient routing protocols.
- Assurance of confidentiality, integrity and availability of the network and its associates for legitimate stations.
- Trust establishment as well as privacy protection for the whole network.
- Future growing network must be designed with adaptive defense mechanism to make it utmost reliable.
- Unconditional effort to curtail the percentage of denial of service attack and its mechanism.
- Highly recommended security architecture designing, its maintenance and regular assessment.
- Authentication with mobility access, easy and secure localization and easy method to discovery the neighbor with appropriate security.
- Always updating the present design of intrusion detection systems.

VII. CONCLUSION

Recent research analyses are presented to provide the idea of security mechanism. Re-keying method has shown the authentication of new node by producing a hash function and confirming by base station. Priority based approach, path based denial of service attack, energy efficient key management, secure topology protocol TLES, virtual certificate authority, lightweight authentication protocol, LEACH based enhanced protocol, intelligent defense mechanism, detection of jammer etc all shown the new approach to increase the security mechanism of wireless sensor network. Recent analytical presentation will help to easy access to work for better protection as well as trustworthy connection. Future work on this issue is a third party authentication for each sensor node or for the new comers to the network with improved key scheduling to stop outsider to get easy access to the network. It will also present that the sensor nodes authorized in the wireless network can become third party authentication server for each other simultaneously and will help the base station to find out intruders and theft.

REFERENCES

[1] Vladimir Dolzhenko, Sergey Klimenko and Alex Leonov; Meshnetics; Industrial Ethernet Book Issue, pp: 38-40, October 2005.http://www.iebmedia.com/index.php?id=5429&parentid=63&themeid=255&showdetail=true

[2] Waltenegus Dargie and Christian Poellabauer, Fundamentals of Wireless Sensor Networks, Wiley Series on Wireless Communicaions and Mobile Computing. pp. 268, ©2010.

[3] E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[4] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, “A Survey Of Security Issues In Wireless Sensor Networks” , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[5] Tanveer Zia and Albert Zomaya, “Security Issues in Wireless Sensor Networks”, IEEE.

[6] Yee Wei Law, “Key Management And Link-Layer Security Of Wireless Sensor Networks”, Ctit Ph.D.- Thesis Series, Series Number: 1381-3617, Ctit Number: 05-75, 2005.

[7] Raymond D.R. Midkiff.S.F, “Denial of Service in Wireless Sensor Network: Attacks and Defenses”, IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, March 2008.

[8] Mohit Saxena, “Security In Wireless Sensor Networks - A Layer Based Classification”, Cerias Tech Report 2007-04.

[9] Hiren Kumar Deva Sarma, Avijit Kar, “Security Threats in Wireless Sensor Networks”, IEEE 2006.

[10] D. Djenouri And L. Khelladi, A.Nadjib Badache, “A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol 7, No. 4 ,Fourth Quarter 2005

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, ICACT, pp: 1043 – 1048, 2006.

[12] Maan Younis Abdullah, Gui Wei Hua and Naif Alsharabi, A Novel Re-keying Function Protocol (NRFP) for Wireless Sensor Network Security. *Sensors* **2008**, *8*(12), 7866-7881, ‘’http://www.mdpi.com/1424-8220/8/12/7866/htm’’

[13] Castro and Liskov, "Practical byzantine fault tolerance," in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[14] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.

[15] Pardeep Kumar and Hoon Jae Lee, Security Issues in Healthcare Application Using Wireless Medical Sensor Networks: A Survey, Sensors, 2012, 12(1), 55-91.

[16] Florin Hutu, Aissa Khoumeri, Guillaume Villemaud and Jean-Marie Gorce, A new wake-up radio architecture for wireless sensor networks, EURASIP Journal on Wireless Communications and Networking, A SpringerOpen Journal, http://jwcn.eurasipjournals.com/content/2014/1/177

[17] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Chaallenges, ICACT Transactions on Advanced Communications Technology 2006, pp: 1043-1048.

[18] Tanveer A. Zia and Albert Y. Zomaya, A Lightweight Security Framework for Wireless Sensor Networks, Journal of Wireless Mobile Networks, Uniquitous Computing and Dependable Applications, Volume: 2, Number: 3, pp. 53-73.

[19] Kuthadi Venu Madhav, Rajendra.C and Raja Lakshmi Selvaraj, Jurnal of Theoretical and Applied Information Technology, pp. 39-44

[20] Kui Ren, communication Security in Wireless Sensor Networks. A Dissertation submitted to the faculty of Worcester Polytechnic Institute in partial fulfillment of the requirements for the degree of doctor of philosophy in Electrical and Computer Engineering, May 2007, pp: 20

[21] Jing Deng, Richard Han, and Shivakant Mishra, Enhancing Base Station Security in Wireless Sensor Networks, University of Colorado, Department of Computer Science Technical Report CU-CS-951-03, April 2003, pp. 15.

[22] Dr. Manoj Kumar Jain, Wireless Sensor Networks: Security Issues and Challenges, IJCIT, Vol. 2, Issue. 1, pp. 62-67

[23] Mark Luk, Ghita Mezzour, Adrian Perrig, MiniSec: A Secure Sensor Network Communication Architecture. In Proceedings of the Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007), April 2007.

[24] Mohammad Hossain, Mohammad Zavid Parvez & Mohammad Hamidul Islam, Mutual Authentication Can Improve the Security of IEEE 802.16 WiMax Network. International Journal of Engineering (IJE), volume 5, issue 4, pp 292 – 301, 2011.

[25] V. Thiruppathy Kesavan, S. Radhakrishnan; Multiple Secret Keys based Security for Wireless Sensor Networks, International Journal of Communication Networks an Information Security (IJCNIS), Vol. 4, NO. 1, April 2012.

[26] Ming Wei Wang, Lie Jun Wang, Qing Hua Yang and Wei Min Xie, Realizing a mutual Authentication Scheme based on Telosb in Wireless Sensor Networks. Journal of Software Engineeing, Vol. 8, Issue. 3, pp. 194-202, 2014.

[27] N. suganthi, V. Sumathy; Energy Efficient Key Management Scheme for Wireless Sensor Networks; International journal of computer and communication, Vol. 9, Issue. 1, pp. 71-78, February, 2014.

[28] Nabila Rahman, Matthew Wright, Donggang Liu; Fast and energy efficent technique for jammed region mapping in wireless sensor networks; asXiv: 1401.7002v1 [cs. NI] 27 January 2014.

[29] Mr. A. babu Karupppiah, A. Raja Pradash; Sybilsecure: an energy efficient sybil attack detection technique in wireless sensor network; international journal of information scinces and techniques (IJIST) vol. 4, no. 3, May 2014.

[30] Somia Sharma, Mr. Kaushik Ghosh, Providing privacy and security of wireless sensor network using ACTOR nodes, Control Theory and Informatics, vol. 4, no. 4, 2014.

[31] P. Sivakumar, K. Amirthavalli and M. Senthil, International Journal of Distributed Sensor Networks, Vol. 2014, Article ID 319587, Hindawi Publishing Corporation May 2014.

[32] Dong Chen, Zhenjiang Zhang, Fan Hsun Tseng, Han Chieh Chao and Li Der Chou, A novel method defends against the path based DoS for wireless sensor network. International journal of distributed sensor networks, vol. 2014, article ID. 654271, July 2014.

[33] Zuo Chen, Min He, Wei Liang and Kai Chen, Trust Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network, Journal of Sensors, Article Id 716468, Hindawi Publishing Corporation, October 2014.

[34] Ayman Tajeddine, Ayman Kayssi, Ali Chehab and Imad Elhajj, Authenticaton Schemes for Wireless Sensor Networks. 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014

[35] Gaurish M. Edake, Ganesh R. Pathak and Suhas H. Patil, Secure Localization and Location

Verfication of Wireless Sensor Network, 2014 4th IEEE International Conference on Communication Systems and Network Technologies, 2014 IEEE.

[36] Ms. Rashmi P. Fulare and Ms. A. V. Sakhare, Efficient sensor node authenticaton in wireless interated sensor networks using virtual certificate authority, 2014 4th IEEE International Conference on Communication Systems and Network Technologies, 2014 IEEE

[37] Shih Chang Lin and Chih Yu Wen, Device based asynchronous ranging and node identification for wireless sensor networks, IEEE Sensors Journal, vol. 14, No. 10, pp. 3648-3662, October 2014.

[38] Manali D. Shah, Shrenik N. Gala and Dr. Narendra M. Shekokar, Lightweight authentication protocol used in wireless sensor network, 2014 IEEE International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA) 2014 IEEE.

[39] Yanhong Sun and Ming tang, A Enhanced Protocol for LEACH Based Wireless Sensor Networks, 2014 International Symposium on Computer, Consumer and Control, pp 344-347 IEEE Computer Society, 2014 IEEE.

[40] Pengfei Hu, Kai Xing, Xiuzhen Cheng, Hao Wei and Haojin Zhu, Information Leaks Out: Attacks and Countermeasures on Compressive Data Gathering in Wireless Sensor Networks, IEEE INFOCOM 2014 – IEEE Conference on Computer Communications.

[41] Jake Bielefeldt and Sriram Chellappan, Sensor Authentication in Collaborating Sensor Networks, 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED – HOC - NET), 2014 IEEE

[42] Zhang Ying and Ji Pengfei, An Efficient and Hybrid Key Management for Heterogeneous Wireless Sensor Networks, 2014 26th Chinese Control and Decision Conference (CCDC) pp. 1881-1885, 2014 IEEE

[43] Ravi Kishore Kodali, Key Management Technique for WSNs, 2014 IEEE Region 10 Symposium, pp. 540-546, 2014 IEEE.

[44] Daehee Kim and Sunshin An, Efficient and Scalable Public Key Infrastructure for Wireless Sensor Networks, 2014 IEEE.

[45] Joao P. amaral, Luis M. Oliveira, Joel J. P. C. Rdrigues, Guangjie Han and Lei Shu, Policy and Network Based Intrusion Detection System for IPv6 Enabled Wireless Sensor Netowkrs, IEEE ICC 2014 – Communications Software, Services and Multimedia Applications Symposium, pp. 1796-1801, 2014 IEEE.

[46] P. Raghu Vamsi and Krishna Kant, Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks, 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT) pp. 698-702, 2014 IEEE.

[47] Zhang Ying and Ji Pengfei, A Kind of Dynamic key Management Method for Sensor Networks, Proceedings of the 33rd Chinese Control Conference, pp. 417-422, July 28-30, 2014, Nanjing, China.

[48] Ismail Mansour, Gerard Chalhoub, Pascal Lafourcade and Francois Delobel, Secure Key Renewal and Revocation for Wireless Sensor Netowork. 39th Annual IEEE Conference on Local Computer Networks, pp. 382-385, LCN 2014, Edmonton, Canada, 2014 IEEE,

[49] E. Sandeep Kumar, S. M. Kusuma and B. P. Vijaya Kumar, An Intelligent Defense Mechanism for Security in Wireless Sensor Networks, International Conference on Communication and Signal Processing, April 3-5, 2014 India, 2014 IEEE.

[50] J. Thangapoo Nancy, K. P. Vijayakumar and Dr. P. Ganesh Kumar, Detection of Jammer in Wireless Sensor Netowork, IEEE International Conference on Communication and Signal Processing, April 3-5, 2014, India.

[51] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh and Ahmad Nassar, Security in Wireless Sensor Networks – Improving the LEAP Protocol. International Journal of Computer Science & Engineering Survey (IJCSES) Vol. 3, No. 3, June 2012

[52] Chintan Gurjar, Hacking, Inforsec Institute, Ref: 877.791.9571, December 23, 2013.