Security Issues and Remedies in Wireless Sensor Networks- A Survey

Rohit Vaid
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207

Vijay Kumar
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207

ABSTRACT
Due to significant advancement in wireless communication, wireless sensor networks (WSNs) have attracted great attention in recent years. WSNs are randomly deployed, battery operated autonomous systems consisting of large number of sensors nodes which are responsible for transmitting the real-time sensed data for a specific application in the monitoring area to the base station where it can be further processed and analyzed. However, due to wireless communication, the network is easily compromised. Solutions dedicated to wire networks are not suited in the resource constrained wireless network. There is still a scope for wide research potential in the field of wireless sensor network security. In this paper, we analyzed the issues related to security in WSNs and also highlight the research area in the field of wireless sensor networks.

Keywords
WSNs, Attack, Security, Constrains, Requirements, Sensor node, Base Station, Characteristics, Forward Secrecy, Backward Secrecy.

1. INTRODUCTION TO WSNs
A wireless sensor network consists of large number of wireless nodes able to take environmental measurements (temperature, light, sound, and humidity). These nodes are small in size but are equipped with sensors, embedded microprocessors and radio transceivers; therefore have not only sensing capability, but also the capability of data processing and communicating capability. The node communicate over a short distance via a wireless medium to accomplish a common task, such as environment monitoring, battlefield surveillance and industrial process control. Fig 1 show a network of wireless sensors which are randomly deployed in the area of interest. The range of every node is very limited, so it can communicate only with those nodes that are within its communication range. In Fig 1 the connectivity of every sensor node with its neighbors that are within the communication range of this sensors are shown with the help of a link. Some nodes are disconnected in the network because they have no connectivity with the network as the network is randomly deployed.

Fig 1 shows a randomly deployed wireless sensor networks in a two dimensional coverage area 'A' that is 100 meter square. This network consists of a set of sensor nodes S = {s_1, s_2,…,s_{100}). Each sensor S_i, i=1..100 located at random coordinate (x_i,y_i) inside 'A'. Each sensor has a sensing range of r_i, i.e. 15 meters. All the sensors will communicate with each other and establish a routing topology to form a single network. They can sense the environmental conditions as a data and then transmit this data back to a collection point known as base station which is shown with ID number 101 at X=50 and y=50 area in Fig 1.

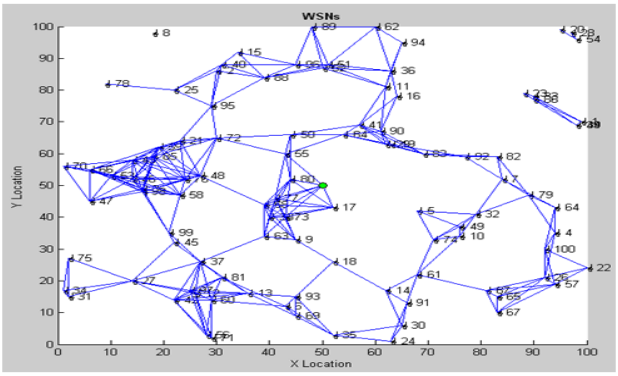

Fig 1: Randomly deployed WSNs

2. CHARACTERISTICS OF WSNs
Wireless sensor networks have the following unique characteristics as shown in Fig 2:

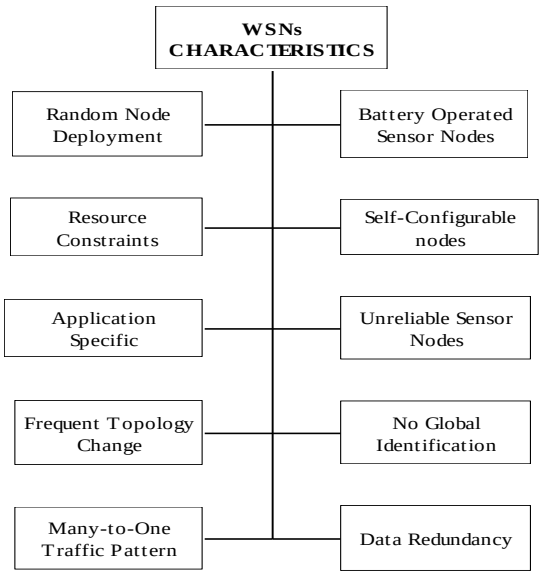

Fig 2: Characteristics of WSNs

- *Random Node Deployment:* Sensor nodes are usually randomly deployed in the interested area without any careful planning and engineering.

- *Battery Operated Sensor Nodes:* Sensor nodes are usually operated by battery to perform any type of operation. It is also

impossible to change or recharge their batteries once they are deployed because in most situations, they are deployed randomly in an unattended environment.

- *Energy, Computation and Storage Constraints:* Sensor nodes are limited in energy, computation, and storage capacities which make it very difficult to implement strong security algorithms.

- *Self–Configurable nodes:* Sensor nodes are usually randomly deployed without careful planning and engineering. Once deployed, sensor nodes have to autonomously configure themselves into the communication network.

- *Application Specific:* A network is usually designed for a specific application and operation. The design requirements of a network are different from one application to other.

- *Unreliable Sensor Nodes:* Due to limited energy and small size of sensor nodes, there are always chances that a node will fail or physically damage. This will be the cause of unreliability in the network.

- *Frequent Topology Change:* Node failure, damage, addition, energy depletion or channel fading is frequently occurring in the network that will result in frequent topology updating in the network.

- *No Global Identification:* Due to the large number of sensor nodes, it is impossible to build a global addressing scheme for the entire network because it would introduce a high overhead for the identification of every sensor.

- *Many-to-One Traffic Pattern:* In most of the sensor network applications, the data sensed by every sensor node is flow from the node in the direction of a Base station, exhibiting a many-to- one traffic pattern.

- *Data Redundancy:* In most of the sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of redundancy.

3. SECURITY CONSTRAINS IN WSNs

A wireless sensor network has many security constraints as compared to a traditional wired network. Due to these security constraints, it is very difficult to directly employ the existing security approaches of wired network into the wireless sensor networks. Therefore, to develop an energy efficient security mechanism, it is necessary to know and understand these security constraints first. In this section, we will discuss security constrains in WSNs shown in Fig 3:

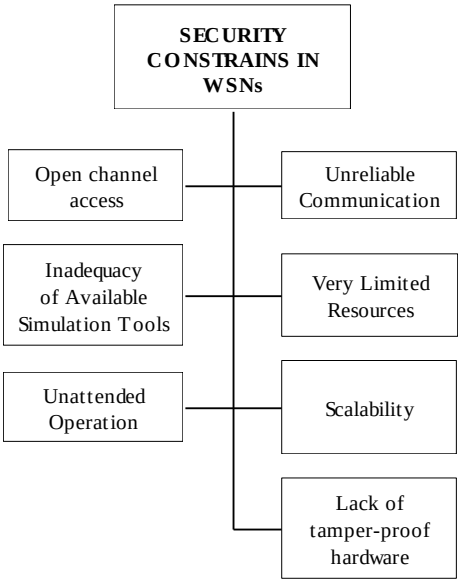

Fig 3: Security constrains in WSNs

- *Open channel access:* Wireless channels are open to everyone. It provides a convenient way for attackers to break into the network. Also most of the protocols used in wireless sensor networks are publicly known. For these reasons, attackers can easily launch attacks by exploiting security holes in the network.

- *Unreliable Communication:* The security of a network depends upon the protocol that depends upon a communication. Even if the protocol is reliable, the communication may still be unreliable. This is due to the open channel access. So a weak radio link will support unreliability in the network.

- *Inadequacy of Available Simulation Tools:* It is very complex task to build a simulator to be used in WSNs. But the solution of this problem is that there are several popular simulators freely available to be used in wireless sensor networks. Some of them are NS-2, TOSSIM, GloMoSim, UWSim, SENS, COOJA, Castalia, Shawn, EmStar, SENSE, VisualSense, OMNeT++, J-Sim, ATEMU and Avrora. But every simulator has its own limitations. Some simulators will support only a limited number of protocols while others are limited to use in IP networks only. It is very complicated to use and learn a simulator as it will take a lot of time. Second thing is that it requires special training to use the simulator. It is an art that is learned with experience over time. So people will like to use a simple language like MatLab as a replacement of simulators.

- *Very Limited Resources:* All the sensors used in the network are resource constrained in terms of memory, energy, processing power and communication bandwidth. So the security protocols used in the traditional wired networks are not compatible with the resource constrained wireless networks.

- *Unattended Operation:* Sensor nodes are usually deployed in an unattended and harsh environment that is open to attackers, hard environments and so on. The chances that a sensor node physically captured in such environments are much higher than the traditional wired network which is located in a secure place in a controlled manner.

• *Scalability:* Traditional security protocols are designed only for point to point settings. So if these traditional protocols are applied in the wireless sensor networks where the number of sensors is very-very large, will add a large number of overheads which are uncontrolled to manage.

• *Lack of tamper-proof hardware:* The size of sensor nodes is so small that it is practically impossible to add a temper-proof hardware unit in the small size sensor node where all the sensitive information like symmetric key or other secrets are stored that are always safe from the adversary by physically capturing the node.

The security services in WSNs are usually centered on cryptography. However, due to the constraints in WSNs, many already existing symmetric or asymmetric key cryptography algorithms such as DES, AES, IDEA, RSA etc are not in use for WSNs. Key distribution is also a problem in symmetric key cryptography algorithms. Similarly permanent unique key stored in each sensor is also not a solution as if the key is compromised then all the future communication and data used by that sensor is compromised. So we need a lightweight encryption algorithm that will use the concept of dynamic key, i.e. the key used by any sensor is update regularly and the problem of key distribution is not required in the network.

4. SECURITY REQUIREMENTS IN WSNs

The basic goal of security in WSNs is to protect the information stored in the memory of sensor and also to keep track of the information and resources from attacks and misbehavior. Security requirements in WSNs are shown in Fig 4.

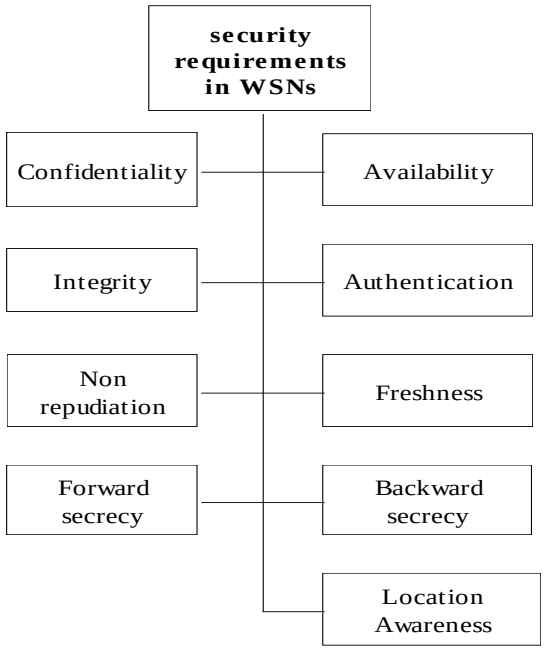

Fig 4: Security Requirements in WSNs

Whenever some malicious node attacks the network then this normal communication will change and the security is compromised. A normal communication between sending sensor 'S' and receiving sensor 'R' is shown in Fig 5.

Fig 5: Normal Communication

• *Confidentiality:* This ensures that the classified data should be accessible and understood only by the authorized sensors. Fig 6 shows a loss of confidentiality. The data is disclosed by the attacker when the data is travelled from sender to receiver over the wireless medium. This attack is known as interception.

Fig 6: Loss of Confidentiality

• *Availability:* This ensures that the desired network services like flow of data in both directions i.e. from sensors to base station and from base station to sensors is available all the time even in the presence of denial-of-service attacks. Fig 7 shows a loss of availability by the attacker to stop using the services given to some authorized sensor 'S' given by the other authorized sensor 'R'. This attack is known as interruption.

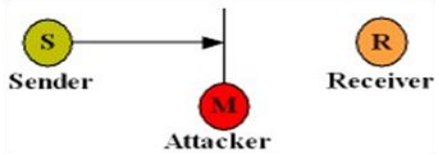

Fig 7: Loss of availability

• *Integrity:* This ensures that changes need to be done in the message only by the authorized sensors and through authorized mechanisms. Or in other words the message is not modified during transmission by malicious intermediate nodes. Fig 8 shows a loss of integrity by the attacker where the attacker has change the ideal route of the message and after change the message send it to receiving sensor. This attack is known as modification.

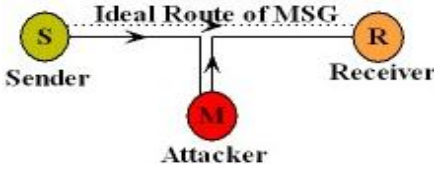

Fig 8: Loss of integrity

• Authentication: This ensures that origin of the received message or packet in the network is correctly identified before using it in the network. Fig 9 shows the scenario where a malicious sensor 'M' will send the information to receiving sensor 'R' to impersonate itself as a sensor 'S'. This attack is known as fabrication.

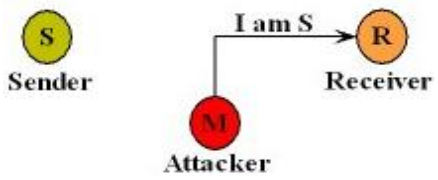

Fig 9: Loss of authenticity

- *Non-repudiation:* which ensures that a node cannot deny sending a message it has previously sent. Fig 10 shows non-repudiation attack where the sender of the message 'S' later deny that it has never sent the message to the receiver 'R'.

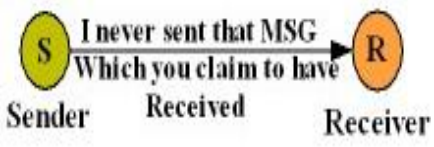

Fig 10: Non-repudiation Attack

- *Freshness:* This ensures that the data is recent and ensures that no adversary can replay old messages. Fig 11 shows replay attack where the attacker 'M' will store packet 'P1' send by the sensor 'S' to sensor 'R' through intermediate sensor 'A' in its memory and later send this stored packet 'P1' to sensor 'A' which will forward this packet one more time to sensor 'R'.

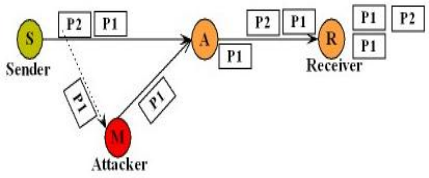

Fig 11: Replay Attack

- Forward secrecy: This ensures that a compromised current secrets or keys should not be able to compromise any secret or key in future.
- *Backward secrecy:* This ensures that a compromised current secrets or key should not be able to compromise any earlier secret or key.

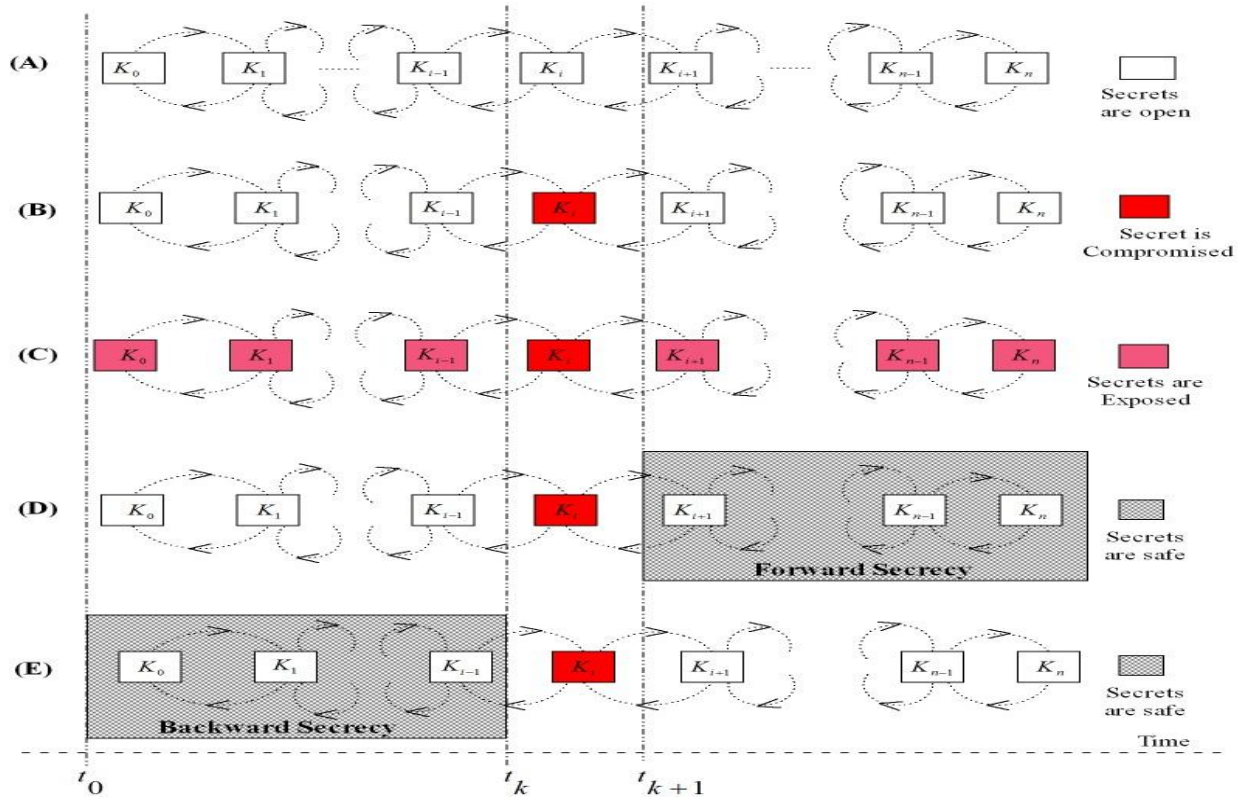

Fig 12: Forward and Backward Secrecy

The concept of forward and backward secrecy is given in Fig 12. Fig 12 (A) shows that the second key (K1) is generated with the help of a first key (K_0) and third key (K_2) is generated with the help of second key (K_1) and similarly K_i is generated with the help of a K_{i-1} key and so on. In Fig 12 (B) a single key (K_i) is compromised at time t_k that result in exposing all keys of the system as shown in Fig 12(C). In Fig 12(D) the concept of forward secrecy is shown which secure all keys that are generated after time t_{k+1}. In Fig 12 (E), the concept of backward secrecy is given which secure all keys by exposing that are generated before time tk when a key has been exposed at time tk.

- Location awareness: This ensures that the damage cannot be spread from the victimized area to the entire network by security attack even if the sensor node is compromised.

5. SECURITY ATTACKS IN WSNs

Sensor networks are vulnerable to several types of attacks. These attacks can be performed in a variety of ways which includes:

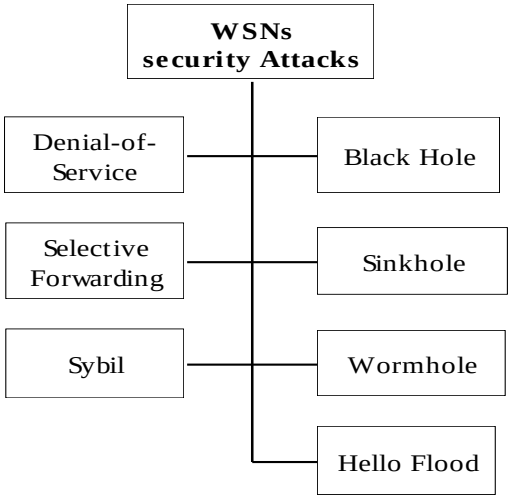

Fig 13: Attacks on WSNs

- Denial-of-Service Attack: In the Denial-of-Service (DoS) attack, a malicious node will attempt to disrupt the network services partially or completely. The result of this attack is that the network will stop functioning or the services of a network will slow down. A variant of Denial-of-Service attack is Distributed Denial-of-Service Attack (DDoS). The functioning of DDoS attack is similar to that of DoS attack. But the difference between both of them is that, in DDoS attack there is more than one attacker, performing DoS activity from different location.

- Black Hole Attack [18]: Black Hole is a region which prevents anything from escaping. In this type of attack, a malicious node will drop all the packets passing through it. Fig 14 shows the working of a Black Hole Attack. In the network shown in the figure, an ID is assign to every node. A malicious node number 37 will discard all the packets that are received by it. Gray shade represents attack area in the figure. In the network malicious node number 37 will position itself on the point where it can receive data send by other nodes (12, 13, 27, 37, 42, 45, 60, 81 and 99). In this case a malicious node will create a Black Hole for these nodes. There are some other nodes (31, 34, 56, 71 and 75) which are aware of this attack but their packets will be passed to base station by other nodes through this path. So overall the packets send by these nodes also lost in the black hole region. We can say that all of these nodes are disconnected from the network.

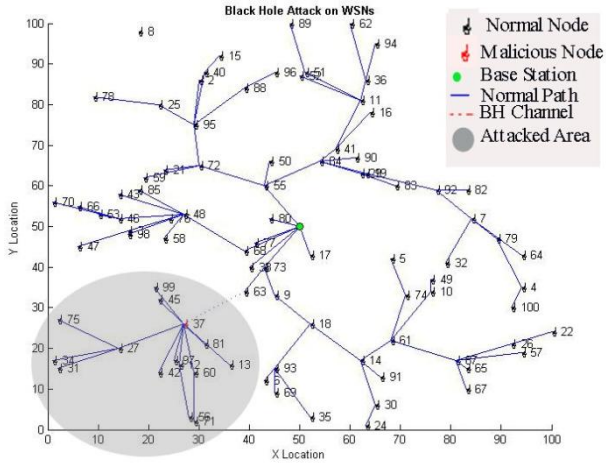

Fig 14: Black Hole Attack

- Selective Forwarding Attack: The functioning of this attack [18] is also similar to that of black hole attack but the difference between both of them is that in selective forwarding attack, instead of dropping all the packets like in black hole attack, the malicious node will drop only those packets that are matched within certain criteria, i.e. drop selected packets of a node or to drop all packets from a selected node. Fig 15 shows the working of a Selective Forwarding Attack. In the network shown in the figure, a malicious node number 18 will discard any packet receive from one path but pass all the packets received from other path. Gray shade in the figure represents the attacked area. Since it is very difficult to distinguish between packet losses due to mobility or channel errors and packet drops due to malicious node. So selective forwarding attack is even harder to detect than black hole attack.

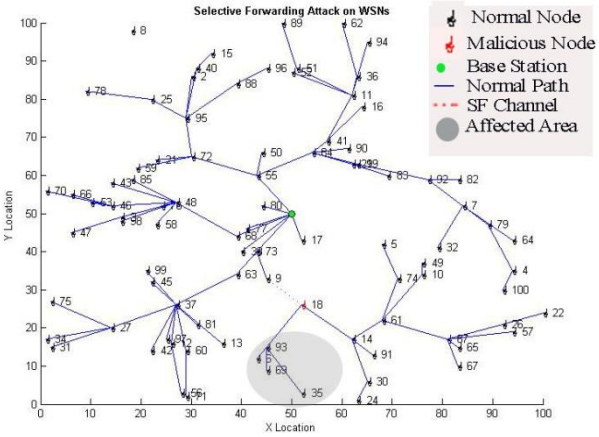

Fig 15: Selective Forwarding Attack

- Sinkhole Attack: In Sinkhole attack [18], a malicious node claims to be a base station. The aim of malicious node is to collect maximum network data by position itself on the point where maximum traffic will flows in the network. The working of Sink Hole attack is shown in Fig 16. A network as shown in figure, a malicious node number 61 pretends to be a sink among its neighboring nodes (74, 87 and 91). The data of neighboring nodes (10, 14, 15, 22, 24, 26, 30, 49, 57, 65 and 67) of these neighbors (74, 87 and 91) is also collected by the malicious node because (74, 87 and 91) nodes are also act as gateway nodes for their neighbors.

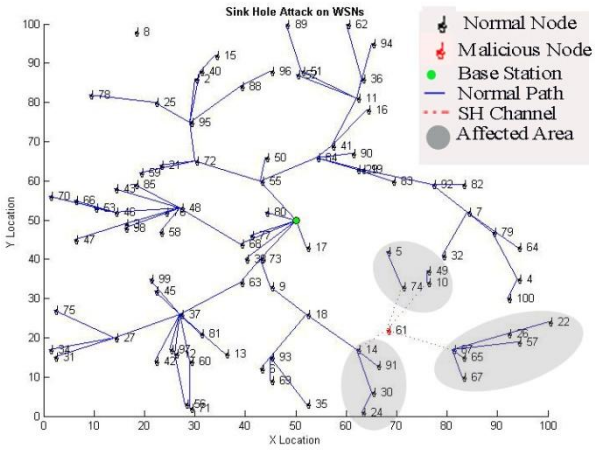

Fig 16: Sink Hole Attack

- Sybil Attack: In this type of attack, a malicious node presents a more than one identity at different locations in the network. Fig 17 demonstrates the working of a Sybil Attack. In the network shown in the figure, malicious node number 37 pretends to be more than one identity at different location in the network.

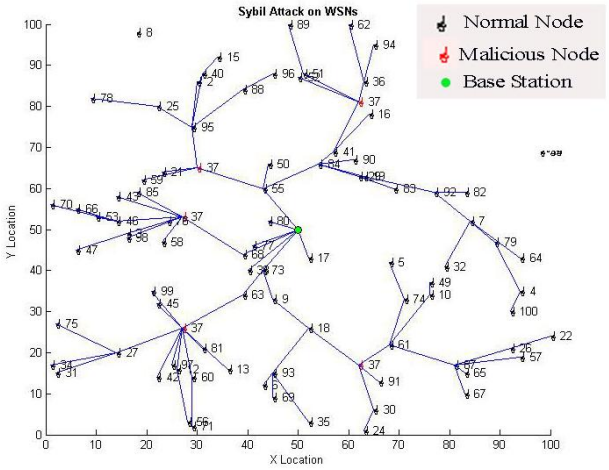

Fig 17: Sybil Attack

- Wormhole Attack: This attack is performed by more than one collaborating malicious nodes. In this type of attack, one malicious node collects packets at some location and tunnels them to another location to other malicious node in the network through a high quality out-of-band link. Other malicious node will further retransmit these packets to some other location in the network. Fig 18 demonstrates the working of a Worm Hole Attack. In the network shown in the figure, malicious node number 40 collects packet at one end and tunnel them to other end at malicious node number 55 which again retransmit these packets to some other location in the network.

- Hello Flood Attack [19]: Many WSNs protocols use the exchange of HELLO messages to update their one hope local neighborhood information. But a powerful malicious node broadcast a single HELLO message to every node in its wide communication range. The result is that every node receiving this HELLO message thinks that the attacker is within one-hop radio communication range to this malicious node.

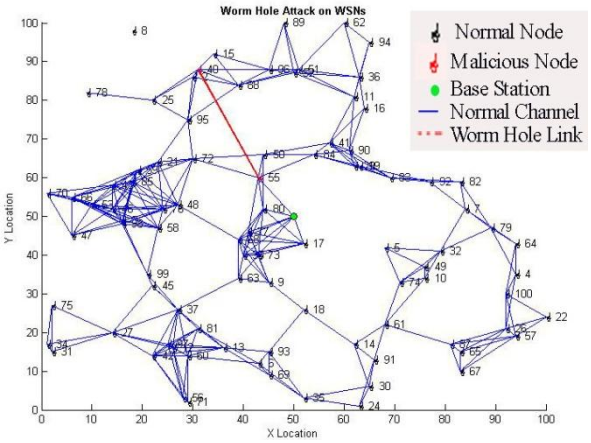

Fig 18: Worm Hole Attack

6. RELATED WORK

Recently, many schemes were proposed to secure the communication in WSNs. This section classifies WSNs security based on the application scenarios, including cryptography, integrity, authentication and key management.

A survey of WSNs security threats affecting different layers along with their defense mechanism is presented in [1]. The major topics in wireless sensor network security architecture framework includes the requirements in the sensor security, classify many of the attacks, listing out their corresponding defensive measures that can be applied, and finally the classification of secure routing protocols, its design issues and their comparison.

Xi Luo et al. [2] propose three schemes to defend against the traffic analysis attacks. Firstly, a random routing scheme (RRS) is proposed to provide path diversity. Secondly, they combine RRS with a dummy packet injection scheme (DPIS) to confuse the adversary by tracing or tracing back the forwarded packet to reach the receiver or source. Finally, an anonymous communication scheme (ACS) is proposed to hide the identities of all nodes that participate in packets transmission. Result confirm the proposed scheme can efficiently defend against traffic analysis attacks, take less delivery time and achieve uniform energy consumption.

Tamara Bonaci et al. [3] address the problem of physical node capture attacks in wireless sensor networks and provide a control theoretic framework to model physical node capture, cloned node detection and revocation of compromised nodes. By combining probabilistic analysis of logical key graphs and linear control theory, they derive a dynamical model that efficiently describes network behavior under attack. Using LQR and LQG optimal control theory tools, they develop a network response strategy, which guarantees secure network connectivity and stability under attack.

Bhoopathy et al. [4] suggested an energy constrained secure hierarchical data aggregation in Wireless Sensor Networks. They divide the network into clusters, each cluster begins with an aggregator and aggregator was connected to sink. Based on distance to sensor nodes and its energy level the aggregator detects the node. Separate keys were distributed to the two levels i.e., sensor node to the aggregator and aggregator to the sink. Whenever a data had to be sent from a sensor node to

another node; initially the sensor node encrypts the data using a key and sends it to the aggregator.

Araujo et al. [5] surveyed about the challenges and open problem in wireless sensor networks. They describe a wide variety of attacks, including communication attack, attack against privacy, node targeted attack, power consumption attack, policy attack and cryptography attack and different security measures available to handle these attacks.

P. Kalyani et al. [6] have proposed a novel method, which uses three algorithms hybrid to achieve the increase in decryption speed, which in turn reduces the energy used for computation and enhances its performance compared with the existing authentication using classical RSA algorithm. The proposed Enhanced Variant of RSA with CRT using Garnera's algorithm to achieve fast decryption speed and provides better performance when compared to the existing RSA. The private key is generated and passed so that the receiver node need not generate it, which consumes more computational cost, power and memory at the decryption stage. They have also done the signing and verification, which avoids the message spoofing attack and enable message confidentiality. Further, the ERSACRT is designed to counter measure to few attacks possible on RSA. They implemented the ERSACRT in java, tested for system parameters like memory, time, speed and efficiency, and compared with that of RSA. Finally, they conclude that the proposed algorithm ERSACRT is efficient and secured along with improved counter measures for secured communication in WSN with reduced energy and computational time.

S. Prasanna et al. [7] presents an overview of the different applications of the wireless sensor networks and various security related issues in WSNs.

Nanrun Zhou et al. [8] has proposed an identity-based key management scheme for wireless sensor networks, where the node identity is used to encrypt the key generating material. The pairwise key is generated by the material ultimately. The security of the proposed scheme is analyzed with the provable security. He has proved by simulation that his scheme is IND-ID-CPA secure against some active attacks such as tampering and impersonation. The storage and communication overheads of his scheme are low enough to fit for wireless sensor networks. Addition and revocation of the nodes with backward-security and forward-security respectively make the scheme more feasible and flexible.

Yuexin Zhang et al. [9] propose an efficient key pre-distribution scheme based on two polynomials in wireless mesh networks by employing the nature of heterogeneity. His scheme realizes the property of bloom filters, i.e., neighbor nodes can discover their shared keys but have no knowledge on the different keys possessed by the other node, without the probability of false positive. The analysis presented in his research shows that his scheme has the ability to establish three different security level keys and achieves the property of self adaptive security for sensor networks with acceptable computation and communication consumption.

Manjusha Pandey et al. [10] have made an effort on residual energy based anti-traffic analysis privacy preservation in WSN. Core functionality of WSN includes routing of the sensed data through predetermined optimized routes to the base station thus producing pronounced traffic near the sink node adding up to the revelation of either location of direction of location of base station. To overcome this revelation of base station the traffic patterns may be disguised by introducing fake packets to the generated traffic of original data. Many anti traffic analysis strategies have been proposed and implements with the objective of attaining traffic uniformity in network. But the inclusion of fake packets adds up communication overhead in the network as a whole. Hence the problem undertaken in the current research effort is to optimize the energy consumption at the node level for fake packet generation.

Xiong et al. [11] proposed a fast and Lightweight Pairing-based Cryptographic Library for Wireless Sensor Networks. They present the first fully functional pairing-based cryptographic library for WSNs. The library has an additional of one identity-based encryption scheme and two short signature schemes. They also proposed several new algorithms and techniques and show that they significantly improve the speed and reduce the memory usage of the library.

Wander et al. [12] presents a comparison of two public-key algorithms, RSA and Elliptic Curve Cryptography (ECC). The requirement for energy efficiency suggests that in most cases computation is favored over communication, as communication is three orders of magnitude more expensive than computation. The requirement also suggests that security should never be overdone. More computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

A generalization of this is the "Q-composite key" scheme [13] which improves the resilience of the network (for the same amount of key storage) and requires an attacker to compromise many more nodes in order to compromise additional communication links. The difference between this scheme and the previous one is that the q-composite scheme requires two nodes to find q (with $q > 1$) keys in common before deriving a shared key and establishing a secure communication link. It is shown that, by increasing the value of q, network resilience against node capture is improved for certain ranges of other parameters.

Author in [14] presents a Key-Management Scheme for distributed sensor. In this scheme they include selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. Before deployment, each sensor node receives a random subset of keys from a large key pool; to agree on a key for communication, two nodes find a common key (if any) within their subsets and use that key as their shared secret key. Now, the existence of a shared key between a particular pair of nodes is not certain but is instead guaranteed only probabilistically (this probability can be tuned by adjusting the parameters of the scheme).

Blom [15] proposed a key pre-distribution scheme that allows any two nodes of a group to find a pair-wise key. The security parameter of the scheme is c, i.e., as long as no more than c nodes are compromised, and the network is perfectly secure. They have used one public matrix and one secret symmetric matrix to construct this scheme. Each node will have the share of those matrixes such that any two nodes can calculate a common key between them without knowing each other's secret matrix share. The problem with this scheme is that if more than c number of nodes is compromised, the whole network will be compromised.

Huang [16] have proposed a Secure Encrypted-Data Aggregation (SEA) scheme in Mobile Wireless Sensor Networks (MWSN) environment. Their design for data

aggregation removes redundant sensor readings, which does not uses encryption and maintains data privacy during transmission. When compared to conventional schemes, their proposed scheme provides security and privacy and duplicate instances of original readings will be aggregated into a single packet; thereby, more energy can be saved. However, there is no integrity in their proposed SEA scheme.

Chan et al. [17] Secure hierarchical in-network data aggregation is guaranteed to identify any manipulation of the aggregate by the adversary beyond what is achievable through direct injection of data values at compromised nodes. In other words, the adversary can never gain any advantage from misrepresenting intermediate aggregation computations. The main algorithm is based on performing the SUM aggregation securely by first forcing the adversary to commit to its choice of intermediate aggregation results.

Rohit Vaid et al. [20] surveyed that existing heavy symmetric key cryptography algorithms such as DES, AES and IDEA used in traditional networks are not suitable in WSNs due to limited resource and computing constraints sensor nodes. Author develops a pairing based encoding scheme (PBES) based on the pairing method. The proposed scheme uses multiple encoding schemes. If this scheme is used with light weight encryption scheme then this scheme is economical in WSNs than using a heavy cryptography algorithm. The key size used in this way to secure the WSNs is very small. Simulation results proves that the scheme is very efficient than any other types of heavy symmetric key cryptography algorithms.

7. DEFENSIVE MECHANISMS

Due to the limited networking solution in wireless sensor networks, there is a still several applications that have not yet been fully investigated in the field of WSNs security. So it is very crucial to identify and authenticate each node participating in the network and all the data delivered to the network. Otherwise it is very easy for a malicious node to modify the collected information or to inject false information into the network. When the information provided by the networks increases, the risk of secure transmission of information over the networks also increases. To achieve the security requirements in wireless sensor networks, it is necessary that proposed mechanism is lightweight in nature for resource constrained wireless sensor networks. So to achieve the above WSNs security challenges the mechanism includes data encryption, secure key management, malicious node detection and Node revocation & replacement scheme. A brief introduction of the solutions that will achieve the described security goals are given below:

- To achieve performance efficiency and reduce resource requirements in wireless sensor networks an encryption mechanism is required in which a message is segmented into parts and each part will participate in encrypting the message. Proposed technique will eliminate the requirement of key distribution and establishment.
- A secret key establishment between the source and destination by multiple communication paths can decrease the risk of path key exposure problem. Therefore, multi-path key establishment solutions are resilient to resist stop forwarding, ensure network availability from connective failure and prevent compromised sensors from knowing the secret in WSNs.
- There is need to develop an efficient and secure data aggregation technique essential for cluster based WSNs for eliminating data redundancy to reduce energy consumption and hence to extend lifetime of the entire network.
- There is need to design an efficient security mechanism that is used to detect malicious nodes in the network. The basic idea of detection of malicious behavior node is to provide. A hop-by-hop authentication based on intelligent biologically inspired sensor nodes is proposed for detecting malicious nodes in WSNs.

8. CONCLUSION

In this paper, we proposed a security issues and there remedies for WSNs. Introduction of wireless sensor networks is described in Section I. Various characteristics of wireless sensor networks are illustrated in Section II. Section III describes the security constrains in wireless sensor networks. Security requirements in wireless sensor networks are given in Section IV. Section V describes the security attacks in wireless sensor networks. Related work in the field of WSNs security has been analyzed in section VI. Section VII describes the defensive mechanisms that are necessary to achieve wireless sensor networks security. It has been concluded that the efficiency of the network in terms of security can be increased by introducing such solutions that are lightweight in nature and also require limited number of calculations and overhead. By using these techniques one can achieve WSNs security along with the efficiency.

9. REFERENCES

[1] Md Abdul Azeem and Dr. Khaleel-ur-Rahman khan, A. V. Pramod, "Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks-Survey", in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[2] X Luo, Xu Ji and Myong-Soon Park, "Location privacy against traffic analysis attacks in wireless sensor networks", in International Conference on Information Science and Applications (ICISA), Vol. 1. Seoul, Korea, pp. 1–6, April 2010.

[3] Tamara Bonaci, Linda Bushnell and Radha Poovendran, "Node capture attacks in wireless sensor networks: a system theoretic approach", in 49th IEEE Conference on Decision and Control (CDC), Vol. 1. Atlanta, Georgia, USA, pp. 6765–6772, December 2010.

[4] Bhoopathy, V. and R.M.S. Parvathi, "Energy Constrained Secure Hierarchical Data Aggregation in Wireless Sensor Networks", in American Journal of Applied Sciences, ISSN 1546-9239, Vol.9, No.6, pp. 858-864, 2012.

[5] Alvaro Araujo, Javier Blesa, Elena Romero and Daniel Villanueva, "Security in cognitive wireless sensor networks - Challenges and open problems", in EURASIP Journal on Wireless Communications and Networking 2012, 2012:48, February 2012.

[6] Kalyani, P. and C. Chellappan., "Enhanced RSA CRT for Energy Efficient Authentication to Wireless Sensor Networks Security", American Journal of Applied Sciences 9 (10): 1660-1667, ISSN 1546-9239, 2012.

[7] S.Prasanna and Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security", in International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 2, Issue-2, May 2012.

[8] Nanrun Zhou, Qiongxi Jiang and Xun Chen, "Identity-based Key Management Scheme with Provable Security for Wireless Sensor Networks", in Journal of Information & Computational Science Vol. 8, No. 14, pp. 3075-3081, 2011.

[9] Yuexin Zhang, Li Xu and Xinyi Huang, "Polynomial-based Key Pre-distribution Scheme in Wireless Mesh Networks", in Journal of Computational Information Systems, Vol. 8, No. 6, pp. 2539–2549, 2012.

[10] Manjusha Pandey and Shekhar Verma, "Residual Energy Based Anti-Traffic Analysis Privacy Preservation in WSN", in I. J. Computer Network and Information Security, pp. 21-29, 2012.

[11] Xiaokang Xiong, Duncan S. Wong and Xiaotie Deng, "TinyPairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks", in Proceedings of the 2010 IEEE Wireless Communications and Networking Conference, IEEE explore Press, Sydney, DOI: 10.1109/WCNC.2010.5506580, pp: 1-6, April 18-21, 2010.

[12] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta and Sheueling Chang Shantz, "Energy analysis of public-key cryptography for wireless sensor networks" in Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, 18Xplore Press, DOI: 10.1109/PERCOM-2005, pp: 324-328, March 8-12, 2005.

[13] Haowen Chan, Adrian Perrig and Dawn Song, "Random key pre distribution schemes for sensor networks", in IEEE Symposium on Security and Privacy, Berkeley, California, ISSN: 1081-6011, Print ISBN: 0-7695-1940-7, pp. 197–213, 11-14 May 2003.

[14] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks", in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47, November 18–22, 2002.

[15] BLOM, R., "An optimal class of symmetric key generation systems", in proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, Eds.): Advances in Cryptology-EUROCRYPT'84, LNCS 209, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, pp. 335–338, 1985.

[16] Shih-I Huang and Shiuhpyng Shieh, "SEA: Secure Encrypted Data Aggregation in Mobile Wireless Sensor Networks", in Proceedings of the International Conference on Computational Intelligence and Security, IEEE Explore Press, Harbin, DOI: 10.1109/CIS.2007.207, pp: 848-852, December 15-19, 2007.

[17] Chan, H., A. Perrig and D. Song, "Secure hierarchical in-network aggregation in sensor networks", in Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, Alexandria, VA, USA, DOI: 10.1145/1180405.1180440, pp: 278-287, Oct. 30-Nov. 03,2006.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", in Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113–127.

[19] Wood, Anthony D. and John A. Stankovic. "Denial of service in sensor networks." Computer 35.10 (2002): 54-62.

[20] Rohit Vaid and Vijay Kumar, "Pairing based Encoding Schemes (PBES) for Secure Wireless Sensor Networks", in International Journal of Computer Applications, Volume 70, No.17, pp. 43-49, ISSN (Online): (0975 – 8887), May 2013.