A Review Cryptographic Data Security for Reliable Wireless Sensor Networks

Ravi Kant1, Dr. Varsha Namdeo2, Dr. Dinesh Kumar Sahu3

1, 2, 3 Dept. of Computer Science Engineering
1, 2, 3 RKDF Institute of Science & technology, Hoshangabad Road, Bhopal, Madhya Pradesh

ABSTRACT

Wireless sensor network is fast emerging technology in which lots work is going to be done. This is used for various real time applications such as military, scientific, weapons sensor, health field, atmosphere monitoring etc. The sensor is cheap in cost and storage but major problem with this is that it has limited battery energy and more vulnerable to security threats such as DOS attack, Sybil attack and wormhole attack etc so to increase the lifetime of the network or lessen the energy consumption and also to prevent the network from various type of threats different researcher proposed and implemented so many algorithms. In this paper, we presents the literature review of different methods with their short comes.

KEYWORDS *: Battery, Security, Threats, Wireless sensor network*

I. INTRODUCTION

The Wireless sensor network (WSN) is a fresh technology rising from an embedded system, sensor technology and wireless networks. The quick deployment, self-organization and fault tolerance characteristics of wireless sensor networks make them a very promising sensing technique for military, environmental, scientific and health applications [1]. Energy capacity and scalability are two greater challenges in Wireless Sensor Networks. For example, the number of nodes in a indiscriminately unfold network needs to be enough high to ensure connectivity. As a result, when network using its maximum transmission power (MTP) and a node may have very large no. of neighbors. Thus, it becomes critical if it tries to store the information about its neighbor. Having more neighbors than the required leads is unnecessary for energy consumption in the network. This problem can be surmounted by using topology organize which controls the set of neighbors of given node. The transmission power can be abridged beside power consumption by cautiously choosing the set of neighbors. Lack of energy efficiency which delays the lifespan of the network is one of the serious issues in the Wireless Sensor Network (WSN) [2]. One of the utmost challenges in WSNs is to secure the sensed information at nodes and during data transmission, which is characterized by the following security objects [3]:

Confidentiality/Privacy: Data must be protected from being captured by adversaries.

Integrity: Integrity refers to the ability to validate the message has not been tampered, transformed or changed while it was on the network.

Authentication: In this need to know if the messages are from the node it claims to be from determining the reliability of message's source.

Availability: It is to verify if a node has the ability to use the resources and the network is accessible for the messages to move on.

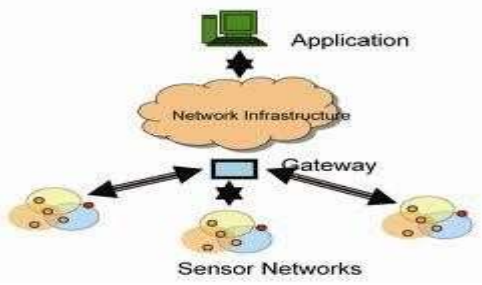

Fig.1 Wireless Sensor Network

In Section II discuss related work for lessening the energy consumption and detecting the security threats on network. The Section III discusses about the routing protocols and Security Attacks. Section IV presents the conclusion about the literature of various method implemented for protection of the energy consumption by the node.

II. RELATED WORK

In this section we discuss methods proposed and implemented by various researchers in field of energy consumption and related to security threats over the network.

M.Sheik Dawood et al [4] proposed the modified QoS enhanced base station controlled dynamic clustering protocol for wireless sensor networks to decreases the energy consumption of node. The simulation results show the better energy consumption is achieved by the proposed protocol when compared to the conventional techniques.

Babak et al [5] proposed an algorithm which makes healthier use of energy and bandwidth which are two restrictions in wireless sensor networks. In the algorithm mobile agent is used to cluster the network and also create the tour to attain collected data from each cluster-head and deliver it back to the sink node. With suitable parameters set, simulation shows that the proposed algorithm exhibits better performance than original direct diffusion in terms of energy consumption [6].

J.Preetheswari et al [7] developed an effective routing mechanism that can with high probability; evade the black hole formed by this attack. The Purely Random Propagation (PRP) algorithm developed produces randomized dispersive routes so that the routes taken by the distribution of different packets changes over time. Besides arbitrariness, the generated routes are also highly dispersive and energy proficient, making them quite capable of bypassing black hole. In addition, the energy constraint is highly optimized in the entire routing method leading to minimal energy consumption. Widespread simulations are conducted to explore the security and energy performance of our mechanism.

Neeraj Kumar et al [8] proposed a secure and energy proficient data diffusion protocol for WSN. A routing metric is defined to prefer the best route from the existing routes. These metric guides those routes to be preferred that consume less energy. Furthermore, for secure data diffusion, a session key is renowned between unlike parties to be communicated. This session key is then used for secure communication between nodes for data diffusion. It is found that the proposed protocol is moderately effective in comparison to the existing protocols with respect to these metrics.

Zhu et al. [9] proposed an interleaved hop-by-hop au- thentication scheme to prevent injection of false data into sensor networks. The proposal makes sure that the BS can detect a false report when no more than a certain number of nodes are compromised.

Przydatek et al. [10] proposed SIA, a framework for secure information aggregation in WSNs which makes use of random sampling strategies for allowing user to infer about the legitimacy of a value. Other efforts have focused on more specific types of attacks.

Yong-ki et al. [11] worked on a new approach for energy efficient data aggregation in sensor networks. A sensor network is self possessed of a huge amount of sensor nodes, which are supply constraints, like limited power. An usual notion to collect data by a sink node is to transmit data from sensor nodes to the sink node by multi-hop. It raised two problems first is the hotspot difficulty, in which the sensor nodes closer to the sink run out of energy nearer than other nodes. As the result, the network lost its service ability, despite of a large amount of residual energy of the other nodes. The next one is that the system generates needless traffic during data transmission for choosing a proper data-sending path. To resolves the problems, authors, propose a new energy balanced and efficient data aggregation scheme for WSNs, called designated path (DP) scheme.

Arabi et al. [12] proposed HERF: A hybrid energy efficient routing using a fuzzy method in Wireless Sensor Networks. Authors work giving attention on Data broadcasting is a significant task performed by WSNs. The algorithms of this system depend on a number of factors such as application areas, practice circumstance, power

and cumulative factors. With respect to these parameters, various algorithms are recommended. An algorithm for hybrid energy efficient routing in wireless sensor networks, which used two algorithms, i.e. EF-Tree (Earliest-First Tree) and SID (Source-Initiated Dissemination) to publicize data and utilizes a fuzzy method to choose group head and to knob between two methods SID and EF-Tree.

M. Nivedita et al. [13] Proposed two keys based method were used. One of the keys is the network-wide key embedded into the nodes prior to their deployment and the other key is the dynamic key. The dynamic key encrypts the message that was primarily encrypted by network-wide key which is a compromised key. Hence, the possibility of attacks to occur is more because the compromised key is used in overall encryption process. Also, this scheme consumes significant amount of energy and memory because the encryption with multiple keys become computationally high.Zhu et al. [14] proposed a key management protocol for sensor networks designed to support in network processing. LEAP solves the problem of key distribution and restricts the impact of a compromised node to the network. LEAP uses four types of keys for each node and communication type. Main drawback of LEAP is the excessive number of messages that must be exchanged during the establishment of keys, thus resulting in the increase of communication cost and energy consumption and limiting the network scalability.

III. ROUTING TECHNIQUES AND SECURITY ATTACK

The efficiency of energy can be improved using some algorithms. That route the data as per network and data communication systems. In this we will some of the energy efficient routing protocols which will be discussed which are LEACH (Low Energy Adaptive Clustering Hierarchy), PEGASIS (Power Efficient Gathering in Sensor Info. Systems) and TEEN (Threshold Sensitive Energy Efficient Sensor Network) etc.

LEACH: Low Energy Adaptive Clustering Hierarchy (LEACH) is a clustering based protocol that uses a randomized rotation of local cluster base stations [15]. LEACH is one of the most popular distributed cluster based routing protocols in WSNs. LEACH is the first and most popular energy efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption and also to increases the lifetime of the network.

PEGASIS : Power-efficient Gathering in Sensor Information Systems [16] is a greedy chain-based power efficient algorithm. Also, PEGASIS is based on LEACH. The key characteristics of PEGASIS are

- The Base Station is preset at long distances from the sensor nodes.
- The sensor nodes are identical and energy constrained with consistent energy.
- No mobility of sensor nodes.

PEGASIS is based on two ideas that are chaining and data fusion. In PEGASIS every node can take twirl of being a leader of the chain where the chain can be created using greedy algorithms that are organized by the sensor nodes. PEGASIS assumes that sensor nodes have a global understanding of the network nodes are motionless (no alliance of sensor nodes) and nodes have locality of information about all other nodes. PEGASIS performs data fusion excluding the end nodes in the chain. PEGASIS better than LEACH by removing the transparency of cluster formation decreases the sum of distances that non leader node have to broadcast less the number of transmissions and receives all nodes and use only one transmission to the BS per round. PEGASIS has the identical problems that LEACH suffers from. Also the PEGASIS does not scale cannot be applied to sensor network where global knowledge of the network is not simple to get. Power Efficient Gathering in Sensor Information Systems (PEGASIS) is an enhancement of the LEACH protocol. Rather than designing multiple clusters it makes chains of sensor nodes so that each and every node transmits and receives from a neighbourhood and only one node is selected from that chain to transmit to the base station. Collected data transfer from node to node, amassed and eventually sent to the base station.

TEEN : Threshold sensitive energy efficient sensor network protocol is used for precipitous changes in the sensed attributes in the network. It uses a data centric mechanism and makes clusters in a hierarchical manner. Two threshold values are transmits to the nodes: hard threshold and soft threshold. The hard threshold is the least promising value of an attribute. Sensor nodes mail data to the cluster head only if they found the sensed value is higher than the hard threshold. If sensor nodes found that the sensed value is less than the feature value

of threshold than they do not send the data to the cluster head. By this way only relative data is send by the sensor nodes. Further; when sensor node again sense value greater than the hard threshold value than they check the difference between current and earlier value with soft threshold. If the dissimilarity is again greater than the soft threshold than the sensor nodes will send recent sensed data to the cluster head. This process will remove encumber from the cluster head [17]

Security Threats in WSN : The WSN is more vulnerable to security threats and it is very necessary to guard our networks from these attacks which are-denial of service, wormhole, hello flood, sinkhole attack.

DENIAL OF SERVICE ATTACK: Denial of Service (DoS) attack is means that not only for the adversary's attempt to subvert, disrupt, or destroy a sensor network, but also for any event that diminishes a sensor network's capability to provide a service [3].In WSNs, several types of Denial of Service attacks in different layers might be performed i.e. at physical layer, the Denial of Service attacks could be jamming and tampering at link layer, confrontation, fatigue, unfairness at network layer, neglect and voracity homing, misdirection and black holes at transport layer this attack could be performed by malicious flooding and resynchronizations [18]. In this attack it abolishes the network's capacity to execute its desired function. The simplest DoS attack tries to ditch the resources required to the victim sensor node, by forwarding additional unwanted message packets and thereby prevents justifiable sensor network users from accessing network resources to which they are endorsed.

SYBIL ATTACK: It is defined as a malicious device illegitimately taking on number of identities. In this Sybil attack, a single sensor node i.e. a malicious sensor device will appear to be a set of sensor devices and it will forward the incorrect message to a sensor node in the network which definitely decreases the normal performance of fault tolerant such as distributed storage, disparity and paths. This incorrect message may be any things [19], which may include the position of sensor nodes, strength; the generation of node which is not actually exists.

WORMHOLE ATTACK: In wormhole attack [20], a pair of attackers forms "tunnels" to transfer the data packets and replays them into the network.
This attack has an incredible effect on wireless networks particularly against routing protocols. Routing method can be baffled and interrupt when routing control messages are tunnelled. It could be formed among the two colluding attackers is referred as wormhole.

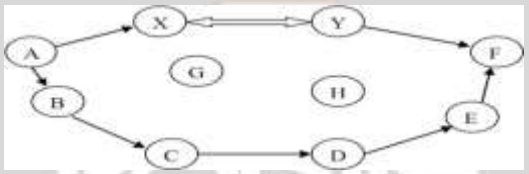

Fig.2 Wormhole Attack

HELLO FLOOD ATTACK: In this, HELLO packets will have high radio transmission range and these are used as weapons in WSN. This processing power sends HELLO packets to a number of sensor nodes which are deployed in a large area within a Wireless Sensor Network. The sensor devices are thus persuaded that the adversary is their neighboring nodes. As a result of this, while forwarding the messages to the base station, the victim sensor nodes try to go through the attacker as they are aware, that it is their neighbours and are spoofed by the attacker [21].

S. No	Security Threats	Preventing Mechanism
1	Denial of Service	Tamper-Proofing and Low Duty Cycle
2	Sybil Attack	Three way handshaking, Route access Limitation
3	Wormhole Attack	suppleness in Routing, False route information detection
4	Hello Flood Attack	False route information recognition
5	Exhausting	Use Spread-Spectrum techniques
6	Jamming	Effective key management schemes

Table 1: Possible attacks and its preventing mechanism in WSN

Table 2: Some of the energy efficient methods of WSN with its effects

S. No.	Methods	Title	Effects
1	Dynamic clustering Protocol	Energy Efficient Wireless Sensor Networks based on QoS Enhanced Base Station controlled Dynamic Clustering Protocol	decrease the energy consumption of node over conventional techniques
2	Distributed Direct Diffusion	Using mobile agent in clustering method for energy consumption in wireless sensor network	enhanced performance than original direct diffusion
3	Purely Randomized Algorithm(PRP)	Optimized Secure Data Delivery based on Randomized Routing in Wireless Sensor Networks	Explore the security , highly dispersive and energy efficient
4	Data Diffusion	A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks	Moderatively effective and less energy consumptive than existing protocol
5	Hop by Hop Authentication Scheme	An interleaved hop- by-hop authentication scheme for filtering of injected false data in sensor networks	prevent injection of false data in the network
6	Secure information Aggregation (SIA)	SIA: Secure information aggregation in sensor networks	Use of random sampling strategies for allowing users to authenticate value
7	hybrid energy efficient routing using a fuzzy method (HERF)	A hybrid energy proficient routing using a fuzzy method in Wireless Sensor Networks, Intelligent and Advanced Systems	More energy competent than EF-Tree

IV. CONCLUSION

The wireless sensor network nodes has limited battery energy and the nodes are also more vulnerable to security attack over the network while many researcher has proposed and implemented different methods and its countermeasures to prevent the network from threats also to improve the battery lifetime but sometimes the it has affected by some other factors so in future the author must need to focus the advancement in battery power and also provide better fault tolerance also protect the sensor network from severe security threats.

REFERENCE

[1] Adil Bashir, Ajaz Hussain Mir, "An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network", International Conference on Advanced Electronic Systems (ICAES) , 2019 in proceeding of IEEE xplore

[2] Subramanian Ganesh, Ramachandran Amutha, "Efficient and Secure Routing Protocol for Wireless Sensor

Networks through SNR Based Dynamic Clustering Mechanisms" Journal of Communications and

Networks, vol. 15, no. 4, august 2018

[3] Luigi Coppolino, Salvatore D'Antonio, Alessia Garofalo, Luigi Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks" Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2019.

[4] K.Parameswari, M.Mohamed Raseen, "Aggregating Secure Data In Wireless Sensor Networks", International Conference on Current Trends in Engineering and Technology, ICCTET'13 in proceeding of IEEE.

[5] Roshan Zameer Ahmed, Anusha Anigol, R. C. Biradar, "Reactive Security Scheme using Behavioral Aspects of Attacks for Wireless Sensor Networks", International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2020, in proceeding of IEEE.

[6] Sudharsan Omprakash, Giridharan Nanthagopal, Santosh Kumar Omprakash, "A secured energy efficient clustering and data aggregation protocol for wireless sensor network", American Journal of Computation, Communication and Control 2019; 1(1): 18-23

[7] Malika BELKADI, Rachida AOUDJIT, Mehammed DAOUI, Mustapha LALAM, "Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks", I.J. Information Technology and Computer Science, 2018, 01, 50-56

[8] BabakNikmard and Salman Taherizadeh, "Using mobile agent in clustering method for energy consumption in wireless sensor network", International Conference on Computer and Communication Technology (ICCCT), pp.153-158, 2020.

[9] Ali K., Neogy S., and Das P.K., "Optimal Energy-Based Clustering with GPS-Enabled Sensor Nodes", Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM), pp.13-18, 2019

[10] Di Tang, Tongtong Li, Jian Ren, Jie Wu, "Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks", Parallel and Distributed Systems, IEEE Transactions 2019 on volume: PP, Issue: 99

[11] Jong-Yong Lee, Kyedong Jung, Hanmin Jung, Daesung Lee, "Improving the Energy Efficiency of a Cluster Head Election for Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2018, Article ID 305037, 6 pages

[12] Fan Wu," incentive-compatible opportunistic routing for wireless networks", mobicom'08, September 14–19, 2008, San Francisco, California, USA 2021

[13] Naveen Sharma, Anand Nayyar, "A Comprehensive Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks", International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 1, January 2020 ISSN 2319-4847

[14] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO in sensor networks," IEEE J. Sel. Areas Communication, vol. 22, no. 6, pp. 1089–1098, Aug. 2020

[15] S. Cui and A. Goldsmith, "Cross-layer design of energy-constrained networks using cooperative MIMO techniques," EURASIP Signal Process. J., vol. 86, no. 8, pp. 1804–1814, Aug. 2021.

[16] M. Dohler, Y. Li, B. Vucetic, A. H. Aghvami, M. Arndt, and D. Barthel, "Performance analysis of distributed space-time block encoded sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 7, pp. 1776–1789, Nov. 2022.