CHAPTER-2

LITERATURE SURVEY

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

This chapter presents an overview of the existing security solutions of general security issues in wireless sensor networks and discusses some recently proposed security protocols.

Rest of the chapter is organized as follows:

Section 2.1 presents related work on security issues and remedies in WSNs followed by the secure data aggregation protocols in Section 2.2. General issues related to key management schemes and existing solutions have been discussed in Section 2.3. A brief description of existing schemes for removing and replacement of compromised sensor nodes from WSNs are given in Section 2.4 followed by the summary of existing protocols to achieve forward and backward secrecy in Section 2.5. Section 2.6 provides the literature related to cryptography in WSNs. Finally, Chapter has been summarized in Section 2.7.

2.1 RELATED WORK ON SECURITY ISSUES AND REMEDIES

Author in [1], presented a survey on security threats and techniques for their defense in WSNs. Authors covered the requirements in sensor security, various attacks and their respective defensive mechanisms, classification of secure routing protocols, design issues and their comparisons for a secure WSN framework.

Xi Luo et al. [2] proposed few techniques in defense against the traffic analysis attacks as under: (i) A Random Routing Scheme (RRS) is presented for path diversity. (ii) RRS and a dummy packet injection scheme (DPIS) are combined together to confuse the adversary by tracing back the forwarded packet to reach the destination. (iii) An Anonymous Communication Scheme (ACS) is presented to secure the identities of all nodes participating in packet transmission.

Author in [3] discussed about the physical node capture attacks in WSNs and proposed a control theoretic framework to handle the problem of physical node capture,

cloned node detection and revocation of compromised nodes. With the help of probabilistic analysis of logical key graphs and linear control theory, authors suggested a dynamical model to describe network behavior under attack. A network response strategy is presented in this work to guarantee secure network connectivity and stability under attack using LQR and LQG tools.

Authors in [4] proposed an energy constrained secure hierarchical data aggregation techniques for WSNs. They proposed the concept of clustered network where each divide the network into clusters, each cluster begins with an aggregator and aggregator was connected to sink. Energy level and the distance to sensor nodes become parameters for aggregator to detect the node. Different keys were distributed to the two levels i.e., one shared between sensor node and the aggregator and other between aggregator and the sink. Whenever data is 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] conducted a survey the challenges and open research areas in wireless sensor networks. This work describes a wide variety of attacks, like communication attack, attack against privacy, node targeted attack, power consumption attack, policy attack and cryptography attack along with different mechanisms to handle these attacks.

Author in [6] proposed a model with hybrid algorithms to speed up the decryption speed and hence to reduces the energy during computation. This technique improves the performance compared with the existing RSA algorithm. The presented Variant of RSA with CRT using Garnera's algorithm achieves fast decryption speed and provides better performance compared to the existing RSA. The private key is generated and passed to avoid re-generation at receiver end and there by consumes less computational cost, power and memory at the decryption stage. Message confidentiality has been maintained through signing and verification by avoiding message spoofing attacks. Further, the ERSACRT is developed to counter measure to the possible attacks 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 concluded that the presented algorithm is efficient and secured along with improved counter measures for secured communication in WSN with reduced energy and computational time.

Author in [7] presented an overview of the various applications of WSNs along with various security issues.

Nanrun Zhou et al. [8] proposed an identity-based key management scheme for WSNs, to encrypt the key generating material using key identity. The pairwise key is generated by the material ultimately. The security of the proposed scheme is analyzed with the provable security. Authors proved that presented scheme is IND-ID-CPA secure against few active attacks like tampering and impersonation. The storage and communication overheads of this scheme are low enough to fit for wireless sensor networks. Addition and revocation of the nodes with backward-security and forward-security make the presented scheme more feasible and flexible in WSNs.

In [9], An efficient key pre-distribution scheme is presented to realize the property of bloom filters where neighbors may find their shared keys but are not aware about the keys possessed by the other node. Analytical results show that this scheme has the ability to establish three different security level keys and achieves the property of self-adaptive security for sensor networks with tolerable computation and communication overheads.

In [10], authors have made an effort on residual energy based anti-traffic analysis privacy preservation in WSN. One of the main function of WSN is routing the sensed packets to the base station through optimized routes thus producing pronounced traffic near the sink node adding up to the declaration of either location or direction of the base station. To overcome this declaration of base station the traffic patterns may be pretended by introducing false 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 false packets increases the communication overhead in the network as a whole

Xiong et al. [11] suggested a library for fast and lightweight pairing based cryptographic scheme in Wireless Sensor Networks. They are the first to present a fully functional pairing-based cryptographic library for WSNs with additional one “identity-based encryption” scheme and two “short signature” schemes. Moreover, this work is supported with some new mechanisms to significantly improve the speed and reduce the memory usage of the library.

Authors in [12] presented a comparative study on RSA and Elliptic Curve Cryptography (ECC). In most of the cases computation is preferred to achieve energy efficiency as communication is about three times more expensive than computation. It is recommended that computationally intensive algorithms should be used to incorporate security due to energy constrains in sensor node.

"Q-composite key" scheme [13] improves the resilience of the network and requires an attacker to compromise many more nodes in order to compromise additional communication links. 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. In this work it is highlighted that by increasing the value of q, network resilience against node capture improves for certain ranges of other parameters.

In [14], a Key-Management Scheme for distributed sensors is presented. This scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. Prior to 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 in probabilistic manner.

Authors in [15] proposed a key pre-distribution scheme to allow any two nodes of a cluster to find a pair-wise key. The security parameter of the scheme is secure as long as no more than the predefined number of nodes are compromised and the network is perfectly secure. In this work, one public matrix and one secret symmetric matrix is used to formally implement this scheme. Each node participates in these matrixes in order to calculate a common key between the two nodes 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.

In [16], a Secure Encrypted-Data Aggregation (SEA) scheme in Mobile Wireless Sensor Networks (MWSN) environment is presented. Their design for data aggregation removes redundant sensor readings, which does not uses encryption and maintains data privacy during transmission. The proposed scheme provides security, privacy and duplicate instances of original readings are aggregated into a single packet to save energy consumption. However, the integrity in this presented SEA scheme is missing.

In [17], a secure hierarchical in-network data aggregation scheme is presented to identify any manipulation of the aggregate by the adversary beyond what is achievable through direct injection of data values at compromised nodes. The adversary never gains any advantage from misrepresenting intermediate aggregation computations. The

proposed algorithm is based on performing the SUM aggregation securely by first forcing the adversary to commit to its choice of intermediate aggregation results.

2.2 RELATED WORK ON DATA AGGREGATION

Author in [20] proposed a communication protocol with significant effect on overall energy dissipation. Author observed that static clustering, multi-hop routing, direct transmission, minimum transmission energy may be optimal for sensor networks. Author also proposed a protocol named as LEACH (low energy adaptive clustering hierarchy) to focus on all these issues. It is a clustering based protocol when utilizes randomized rotation of local cluster base station to evenly distribute energy load in sensors. In LEACH, coordination among the sensors is used for scalability and robustness of dynamic network and apply data aggregation in a manner to reduce minimum data at base station and hence save the network energy.

In [21], classification of the different aggregation techniques designed to achieve some important objectives e.g. reducing data size, minimizing transmission energy, enhancing accuracy, etc. is presented followed with state of the art literature survey of aggregation techniques used in distributed manner to improve lifetime and energy conservation of wireless sensor networks.

A framework for aggregation has been presented in [22] which act as a middleware in this process of measuring and aggregating data from the nodes within the network. This work attempts to collect and aggregate the information in a manner to increase the network lifetime.

In [23], author describes an approach in which nodes in the route contributes some fake aggregated values to secure against possible attacks. The work is supported by a novel algorithm used for verification to enable base station to decide about the contribution in computed aggregate false value.

Vaibhav Pandey et al. in [24] explained the various data aggregation algorithms for WSNs to increase the lifetime of sensor network by reducing the number of packets for onward transmission to the base station. Authors explored the data aggregation algorithms keeping in mind the network topology and then explore various tradeoffs in data aggregation algorithms along with highlights on security issues in data aggregation.

Seyit A. Camtepe et al. [25] explains the three approaches for key distribution problem in WSNs: probabilistic, deterministic, or hybrid. In the probability based

solutions, key-chains are selected randomly from a pool of key and distributed to sensor nodes. In deterministic solutions, deterministic processes are used to design the key-pool and the key-chains for better key connectivity. Finally, mixed solution known as hybrid one uses schemes based on probability theory on the solutions based on deterministic approaches to enhance scalability and resilience.

Authors in [26] presented a scheme known as pre- distribution scheme to partition deployment area in overlapping groups with the help of knowledge of deployment of the network. In this work, there is significant improvement with respect to the network resilience without compromising with connectivity or communications overhead. Simulation results show that there is significant improvement in the performance over the existing mechanisms defined on the basis of deployment knowledge.

In [27], a key management scheme deterministic in nature, called DKS-LEACH, to secure leach protocol against malicious attacks id revealed. Authors design and performed a theoretical evaluation of their security model to secure the setup and study phases of leach protocol. The performance of system is evaluated using TOSSIM simulator. This prevents electing an unwanted and trustless cluster head and different types of attacks from malicious nodes as well.

2.3 RELATED WORK ON KEY MANAGEMENT

Recently, many schemes were proposed to secure the communication in WSNs. In this section, we present a brief overview of the related works used to enhance the security in wireless sensor networks.

In [28], the author introduces a virtual energy based encryption and keying scheme which is also energy efficient also WSNs. The proposed scheme reduces the number of transmissions needed for rekeying to avoid key hacking. The key used in the encryption process changes frequently as a function of the residual virtual energy of the sensor where one time dynamic key is used for one packet and is different for the successive packets in the entire data stream. The intermediate nodes along the path to the sink are capable enough to verify the authenticity and integrity of the incoming packets with the predicted value of the key generated by the sender's virtual energy, thus requiring no need for specific rekeying messages. But synchronization is a big issue in this scheme and once virtual energy is unsynchronized, the packets can't be decrypted.

The result of un-decrypted packet makes is completely impossible to differentiate between authenticated and malicious nodes.

In [29], authors address pair-wise and triple key establishment problems in wireless sensor networks. The scheme presented in [6] is highly resilient against node capture attacks and is applicable for mobile sensor networks while preserving low storage, computation and communication requirements. Author proposed the concept of key distribution in triplicate where all the three nodes share common keys for secure forwarding and detecting malicious nodes with key management in clustered sensor networks. The scheme is based on polynomial and a combinatorial approach for triple key distribution.

In [30], the authors presented an efficient key distribution scheme useful to secure data-centric routing protocols. The scheme presented is an attempt to secure key distribution in centralized manner to provide a multi-level hierarchical organization in WSNs. The scheme key distribution locally for establishing group key and pair wise Key. These two types of keys are very useful to secure data request diffusion and data forwarding through multi-hop routing paths. The scheme is most suited in the networks with dynamic topology.

In [31], the authors proposed a lightweight public key infrastructure known as cluster based public infrastructure (CBPKI), based on the security and the authenticity of the base station for executing a set of instructions meant for establishing a session key between the base station and sensor nodes to ensure data confidentiality and integrity.

2.4 RELATED WORK ON KEY UPDATION FOR REMOVAL & REPLACEMENT OF COMPROMISED SENSOR NODES

Authors in [32] proposed TENCR (Trust Evaluation method based on the Node's QoS Characteristics and neighboring node's Recommendations). This scheme detects malicious and selfish nodes through arithmetic means to allow only trustworthy nodes in routing by eliminating malicious/selfish nodes automatically from the network.

Author in [33] presented trust estimation method to detect compromised sensor nodes from wireless sensor networks. In this scheme, each cluster head periodically broadcasts a request within its cluster to estimate global trust for its members. Provisions have been made for the base station to maintain a record of past interactions with cluster

heads and estimates trust for the cluster heads. In order to determine the current status of the node, the proposed algorithm employs previous trust values and current measured misbehavior components. The given components are combined to obtain a robust trust value. Theoretical analysis and evaluation results prove that proposed scheme is better than other trust schemes given in the proposed literature in terms of detecting an on-off attack and persistent misbehavior.

Authors in [34] proposed an algorithm for trust calculation based on behavior strategy in order to identify selfish and malicious nodes to solve the security problems for node failure in WSNs. Proposed algorithm establishes trust factors by considering network's practical application environment in order to make both quantitative and qualitative analysis for calculating the direct and indirect trust values. In this work, it has been considered that nodes behaviors characterizes a variety of trust factors and coefficients defined with respect to the network applications established to get trust values achieved directly or indirectly through the calculations of weighted average of the trust factors to finally integrated trust value of nodes. The simulation results show that this scheme effectively identifies malicious nodes and reflects the characteristic of trust.

Authors in [35] proposed a scheme or removing compromised sensors from WSNs. This scheme, KeyRev, uses key updation techniques to change the keys owned by the compromised sensor nodes. In this way it removes the compromised nodes from the network. The simulation results prove that this scheme is scalable and efficient in comparison with other key revocation schemes in wireless sensor networks.

Research work in [36] proposes a new trust management scheme for the detection of unexpected node by considering the behaviors of sensor nodes, direct and indirect trusts based on Geometric Mean (GM) of the QoS characteristics among the nodes. These scheme first figures out the malicious nodes in the network and then separates them from the benevolent nodes on the basis of trust levels assigned to them. This way only the trusted nodes are participate in routing messages.

Authors in [37] proposed a secure localization mechanism to detect malicious nodes. In the proposed scheme, all nodes play the role of verifier, by generating local map, i.e. a view constructed based on ranging information from its neighbors. Simulation results prove that proposed scheme is effective in the presence of a large number of phantom nodes.

Research work in [38] proposed geographic routing (GR) protocols to address the attacks falsifying the location information. In GR, neighbors exchange the information about their location. Based on this knowledge, a node forwards packets to its neighbor closest to the destination.

Authors in [39] developed a location-based keys authentication scheme to find the impact of compromised nodes to their vicinity. Proposed research work presents an efficient technique to establish a shared key between any two sensor nodes in the network.

Research work in [40] presents a proximity-based event detection scheme. The proposed scheme is a mixed scheme to take advantages of both the cluster and neighbor oriented schemes to distinguish events from fake alarms. Simulation results prove that proposed scheme improves the performance by removing identified faulty nodes from the network during normal operation.

Authors in [41] proposed a secure and efficient data aggregation scheme in terms of energy for detecting the malicious nodes with invariable communication overheads for each sensor node. In this scheme, the results obtained after aggregation process are sealed with the private keys of the various aggregators to provide integrity and confidentiality. Each node also verifies the aggregation results from its parent.

2.5 RELATED WORK ON FORWARD AND BACKWARD SECRECY

Authors in [42] presented a self-healing key distribution scheme. The proposed scheme is used for secure multicast group communications in WSNs. In this scheme, nodes are capable enough for recovering lost session keys at their own, without requesting any additional transmission from the group controller. In this scheme, all messages meant for rekeying are sent with no encryption using one-way hash function and XOR operation. The proposed scheme supports both the backward and forward secrecy.

Authors in [43] proposed a protocol for the key establishment. This protocol assures forward and backward secrecy of the session key. Proposed work describe that if any set of the session keys gets compromised, including the current session key, these compromised keys neither predict the security of future session keys, nor past history of the session keys.

Authors in [44] developed a technique for unattended sensors to recover from intrusions by soliciting help from peer sensors. Authors proposed certain defense mechanisms to be used in sensors re-gaining secrecy and authenticity of collected data, despite adversary's efforts to the contrary. Analytical and simulation results support their observations and demonstrate for the effectiveness of proposed techniques.

Authors in [45] proposed a distributed group rekeying scheme. This scheme does not require any secure server for rekeying operation. The proposed scheme is based on local collaboration of group members. Simulation results show that comparing with other distributed schemes, the proposed scheme consumes less energy and lower communication overhead.

Authors in [46] proposed forward secrecy scheme and its applications for the future mobile communications security.

In [47], authors proposed a distributed self-healing scheme (POSH) for Unattended Wireless Sensor Networks (UWSNs). The research work presents a new threat model where a mobile adversary periodically compromises and releases sensors. The aim of this adversary is to maximize its knowledge based on collected data. In this scheme, a self-healing protocol is defined that allows sensors to continuously and collectively recover from compromise state.

Authors in [48] define Forward & Backward Secure Key Management in Wireless Sensor Networks for Process Control Systems (PCSs) and Supervisory Control and Data Acquisition (SCADA) systems. In the proposed work, a key management scheme is presented to defeat node captured attack by offering both forward and backward secrecy.

Authors in [49] presented a simple protocol for secret maintenance between a pair of network neighbors. The scheme shows that if the current secret between the pair is disclosed by any reason, past and future secrets are still safe and are never being compromised.

2.6 RELATED WORK ON CRYPTOGRAPHY

Recently, many schemes were proposed to secure the communication in WSNs. This section classifies WSNs security based on the application scenarios.

In [50], authors presented a technique to minimize energy consumption by facilitating the frame header robust to the errors. Simulation result shows that if the

accuracy is to be maintained in the network, the sensor nodes transmit a frame at a lower signal-to-noise-ratio and thus the power consumed by the transmit amplifier is reduced.

S. P. fletschinger et al. [51] considers the application of a network coding scheme in wireless sensor networks for robustness. In this research, network coding in WSN is evaluated in terms of reliability improvement, energy efficiency and resilience to network protocol failures. The proposed model concentrates on the evaluation of coding schemes that takes the advantage of the spatial diversity inherent in different layers of the communication protocol.

In [52], authors presented a scheme to compress the data without any loss using multiple code options. Authors demonstrated the merits of the proposed compression algorithm in comparison with other compression algorithms for WSNs.

Jin Wang et al. [53] address the modeling and design of linear network coding for reliable communication against multiple failures in wireless sensor networks. Proposed work is an attempt to design a deterministic linear network coding scheme based on the average number of path failures simultaneously happening in the network other than the maximum number of path failures. This scheme significantly improves the network throughput in comparison with the traditional approaches. Simulation results demonstrate the effectiveness of the proposed schemes.

Research in [54] considers the distributed classification problem in wireless sensor networks. Based upon local decisions made by the sensors, possibly in the presence of faults, are transmitted to a fusion center through fading channels. Proposed scheme provides performance classification degraded due to the fading channels and malicious sensor nodes. The proposed scheme explores soft decision and local decision rules with no redundancy.

In [55], efficient coding techniques have been used to enhance the throughput of the network without affecting the lifetime. Simulation results prove that throughput increases with the increase in coding rate.

2.7 SUMMARY

In this chapter, state of the art literature review on security issues and data aggregation in WSNs has been presented. This chapter presents the background for the subjects of key management and encryption schemes used in WSNs. In the next chapter, energy efficient secure data aggregation scheme for WSNs has been presented.