Secure Data aggregation Issues in Wireless Sensor Network: A Survey

Priyanka K. Shah and Kajal V. Shukla

Abstract—The research advances and applicability of wireless sensor networks (WSNs) have introduced many new promising applications including habitat monitoring, battlefield surveillance and target tracking. The energy consumption is the major issue to be considered for WSNs which is occupied by data communication among nodes in maximum proportion. Many sensor applications collect data from an individual node which is aggregated at a base station. To reduce energy consumption, in-network aggregation can be performed at intermediate nodes enroute to the base station. As wireless sensor networks are usually deployed in remote and hostile environments to transmit sensitive information, sensor nodes are prone to node compromise attacks and security issues such as data confidentiality and integrity are extremely important. Hence, wireless sensor network protocols, e.g., data aggregation protocol, must be designed with security in mind. The paper investigates the relationship between security and data aggregation process. In this paper general security issues in WSNs have been explored and we present an extensive study to provide a comprehensive review of the existing literature on techniques and protocols for in- network aggregation in wireless sensor networks and analyze possible security threats on them.

Index Terms— Data Aggregation, Security, Threat Model, Wireless Sensor network

1 INTRODUCTION

THE wireless sensor network is an ad-hoc network. It consists of small light weighted, low powered wireless nodes called sensor nodes with limited memory, computational, and communication resources [1],[2] and it measures physical parameters such as sound, pressure, temperature, and humidity. These sensor nodes deployed in large or thousand numbers and collaborate to form an ad hoc network capable of reporting to data collection sink (base station). Sensor networks are increasingly deployed for applications such as wildlife habitat monitoring, forest fire prevention, and military surveillance [3],[4],[5]. In these applications, the data collected by sensor nodes from their physical environment need to be assembled at a host computer or data sink for further analysis. Typically, an aggregate (or summarized) value is computed at the data sink by applying the corresponding aggregate function, e.g., MAX, COUNT, AVERAGE or MEDIAN to the collected data. In large sensor networks, computing aggregates in-network, i.e., combining partial results at intermediate nodes during message routing, significantly reduces the amount of communication and hence the energy consumed. In wireless sensor networks, the benefit of data aggregation increases if the intermediate sensor nodes perform data aggregation incrementally when data are being forwarded to the base station. However, while this continuous data aggregation operation improves the bandwidth and energy utilization, it may negatively affect other performance metrics such as delay, accuracy, fault-tolerance, and security [6].

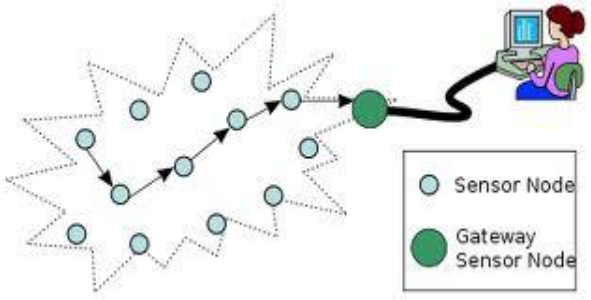

Fig.1. Sensor Network Architecture

As the majority of wireless sensor network applications require a certain level of security, it is not possible to sacrifice security for data aggregation. WSNs are vulnerable to security attacks due to the broadcast nature of radio transmission. Sensor nodes may also be physically captured or destroyed by the enemies. In such large scale wireless sensor networks, neighbouring sensor nodes often have overlapping sensing ranges and therefore they sense the same phenomenon which results in production of large volumes of redundant data. In addition, there is a strong conflict between security and data aggregation protocols. Security protocols require sensor nodes to

encrypt and authenticate any sensed data prior to its transmission and prefer data to be decrypted by the base station [7],[8]. On the other hand, data aggregation protocols prefer plain data to implement data aggregation at every intermediate node so that energy efficiency is maximized. Moreover, a data aggregation result in alterations in sensor data and therefore it is a challenging task to provide source and data authentication along with data aggregation. Due to these conflicting goals, data aggregation and security protocols must be designed together so that data aggregation can be performed without sacrificing security. The necessities of implementing data aggregation and security together have led many researchers to work on secure data aggregation problem.

The aim of the paper is to provide an extensive overview of secure data aggregation concept in wireless sensor networks by defining the main issues and covering the most important work in the area. Our major contributions are to provide the basic architecture for WSN and in-network aggregation process, to define various security requirements, and to classify existing solutions in this area. Rest of the paper is organized as follows. Section 2 gives general overview of the process, functions and categorization of data aggregation. Section 3 defines different security threats and security requirements for WSNs. Section 4 elaborate possible attacks against WSN in general. In section 5, we explore existing WSN data gathering protocols and security threats on them and finally section 6 concludes the paper.

2 DATA AGGREGATION IN WSN

Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced. An example data aggregation scheme is presented in Fig. 2 where a group of sensor nodes collect information from a target region. When the base station queries the network, instead of sending each sensor node's data to base station, one of the sensor nodes, called data aggregator, collects the information from its neighbouring nodes, aggregates them (e.g., computes the average), and sends the aggregated data to the base station over a multihop path.

- *P.K.Shah is with the Charotar Institute of Computer Application, CHARUSAT, Changa.*
- *K.V.Shukla is with the Charotar Institute of Computer Application, CHARUSAT, Changa.*

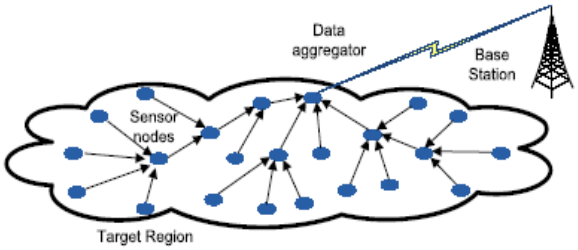

Fig.2. Data Aggregation in WSN

Sensor applications can be broadly classified into two categories depending on the data acquisition systems. Query based system, In query-based systems the base station (the data sink) broadcasts a query to the network and the nodes respond with the relevant information.

Event-based systems, in event-based applications nodes send a message to the base station only when the target event occurs in the area of interest. Sensor systems can also be categorized based on how data is aggregated. In *single- aggregator* approaches, only sink node performs aggregation. Opposite to that, in *hierarchical aggregation* systems, network consists of data aggregator nodes which perform in-network aggregation and enroute to the base station.

Hierarchical approach can be further classified depending upon the routing strategy used by network. *Tree based approaches* use the simplest way to aggregate data flowing from the sources to the sink is to elect some special nodes which work as aggregation points and define a preferred direction to be followed when forwarding data. Similarly to tree-based algorithms, *cluster-based schemes* also consist of a hierarchical organization of the network. However, here nodes are subdivided into clusters. Moreover, special nodes, referred to as cluster-heads, are elected in order to aggregate data locally and transmit the result of such an aggregation to the sink. *Multipath approaches* resolves issues with the previous strategies, it allows nodes to propagate duplicates of same information to multiple neighbours. *Hybrid data aggregation* schemes make use of both the tree based schemes and multi path approach to route aggregated data.

There are two approaches to perform in-network aggregation. In-network aggregation can be done with size reduction and without size reduction. The in-network aggregation with size reduction performs some operation on data collected from various nodes and the other strategy for in-network aggregation performs

merge operation on data, thus does not reduce size of packet but still reducing network traffic. There are several types of aggregation functions exist and most of them are closely related to the specific sensor application. Nevertheless, we can identify some common paradigms for their classification:

- **Lossy and Lossless:** Aggregation functions can compress and merge data according to either a lossy or a lossless approach. In the first case the original values can not be recovered after having merged them by means of the aggregation function. In contrast, the second approach (lossless) allows compressing the data by preserving the original information.
- **Duplicate Sensitive and Duplicate Insensitive:** An intermediate node may receive multiple copies of the same information. In this case, it may happen that the same data is considered multiple times when the information is aggregated. If the aggregation function in use is duplicate sensitive, the final result depends on the number of times the same value has been considered. Otherwise, the aggregation function is said to be duplicate insensitive. For instance, a function that takes the average is duplicate sensitive, whereas a function that takes the minimum value is duplicate insensitive.

3 SECURITY ISSUES IN WSNS

3.1 Security Requirements for Data Aggregation

A sensor network is a special type of ad hoc network. So it shares some common property of traditional networks. The security requirements [9],[10],[11],[12] of a wireless sensor network can be classified as follows:

- Data Confidentiality: ensures that secrecy of sensed data is never disclosed to unauthorized parties. It can be divided into a hop-by-hop basis and end-to-end basis. In the hop-by-hop basis, any aggregator point needs to decrypt the received encrypted data. On the other basis, the aggregator does not need to decrypt and encrypt data; it needs to apply the aggregation functions directly on the encrypted data.
- Data Integrity and Freshness: Data integrity guarantees that a message being transferred is never corrupted. It ensures that the content of a message has not been altered, either maliciously or by accident. Data freshness ensures that the data are recent and no old messages have been replayed.
- Source Authentication: Entity authentication and data authentication are two types of authentications. Entity authentication verifies the receiver whether they are allowed to receive messages or not. Data authentication guarantees that the reported data is the same as the original one.
- Data Availability: ensures that network is alive and data is accessible. The compromised node (attacker) may consume the energy of network. There are two mechanisms to ensure reasonable level of data availability:
  - Self-healing and self organizing that can diagnose, and react to attacker's activities, and also conduct key management and build trust relations among sensor nodes.
  - Aggregator rotation that rotates the aggregation duties between honest nodes to balance the energy consumption in WSN.
- Secure Localization: The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate nonsecured location information by reporting false signal strengths and replaying signals, etc.

3.2 Classes of Security Attacks

- Attacks on the computer system or network can be broadly classified [13] as interruption, interception, modification and fabrication
- Interruption is an attack on network availability, for example physical capturing of nodes, insertion of malicious nodes.
- Interception is an attack on confidentiality. Compromised node can gain unauthorized access to sensor nodes data.
- Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it
- Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

3.3 Adversarial Model

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an

attack. Data aggregation is threaten by two types of adversaries:

- Passive adversary: it takes the advantage from the communication aspect of WSN and eavesdrops on the traffic to obtain any important information about the sensed data. They can also be classified as sensor class or mote class attackers.
- Active adversary: it interacts with the WSN by injecting packets, destroying nodes and so on. They are the laptop class attackers and more powerful, yet affecting much traffic of WSN.

Adversaries can have total or partial access to network and the level of access will affect the security requirements for WSN. Another model can be derived as external threat model and internal threat model. External threats may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise Denial of Service (DoS) attack. Whereas inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile. Insider attacks may be mounted by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes

4 POSSIBLE ATTACKS ON WSNS

4.1 Types of Attacks against WSN

WSNs are vulnerable to different types of attacks due to the nature of the transmission medium (broadcast), remote and hostile deployment location, and the lack of physical security in each node. In this section, these attacks [14], [15], [16], [17] ,[18] ,[19] ,[20], [21] ,[22] ,[23],[24] that might affect the aggregation in the WSN are discussed.

- Denial of Service Attack (DoS): is a standard attack on the WSN by transmitting radio signals that interfere with the radio frequencies used by the WSN and is sometimes called jamming. DoS can be an aggregator that refuses to aggregate and prevents data from travelling into the higher levels.
- Spoofed, altered, or replayed routing information: This is the most common direct attack against a routing protocol. This attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.
- Selective Forwarding Attack: it is assumed in WSN that each node will accurately forward received messages. However, a compromised node may refuse to do so. It is up to the adversary that is controlling the compromised node to either forward the received messages or not.
- Sybil Attack: is where the attacker is able to present more than one identity within the network. It creates multiple identities to generate additional votes in the aggregator election phase and select a malicious node to be the aggregator; also the aggregated result may be affected if the adversary is able to generate multiple entries with different readings.
- Node Compromises: also known as sinkhole attack. By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node. A compromised node which is placed at the centre of some area creates a large “sphere of influence”, attracting all traffic destined for a base station from the sensor nodes.
- Wormhole Attack: In this attack an adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbours, leading to quick exhaustion of their energy resources.
- HELLO Flood Attack: Many protocols require nodes to broadcast HELLO packets for neighbour discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbour, so that all the nodes will respond to the HELLO message and waste their energy.
- Acknowledgement Spoofing: Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for “overheard” packets addressed to neighbouring nodes. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing.

- Sniffing Attack: Sniffing attack is a good example of interception or listen-in channel attack. In this attack an adversary node is placed in the proximity of the sensor grid to capture data. The collected data is transferred to the intruder by some means for further processing. This type of attack will not affect the normal functioning of the protocol. An outside attacker can lunch this attack for gather valuable data from the sensors.
- Data Integrity Attack: It is a stealthy attack that compromises the data travelling among the nodes in WSN by changing the data contained within the packets or injecting false data. The attacker node must have more processing, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor data and by doing so compromise the victim's research.
- Energy Drain Attack: WSN is battery powered and dynamically organized. It is difficult or impossible to replace/recharge sensor node batteries. Because there is a limited amount of energy available, attackers may use compromised nodes to inject fabricated reports into the network or generate large amount of traffic in the network. Fabricated reports will cause false alarms that waste real world response efforts, and drain the finite amount of energy in a battery powered network.
- Black-hole Attack: The black hole attack positions a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This attack can isolate certain nodes from the base station and creates a discontinuity in network connectivity.
- Node Replication Attack: This is an attack where attacker tries to mount several nodes with same identity at different places of the existing network. There are two methods for mounting this attack. In first method the attacker captures one node from the network and creates clone of a captured node and mounts in different places of the network. In second method attacker may generate a false identification of a node then makes clone out of this node and mounts in different places of the network. These mounted clone nodes tries to generates false data to disrupt the network.

4.2 Layering based Attacks

Though there is no such standard layered architecture of the communication protocol for wireless sensor network, here we have summarized possible attacks and their security solution approaches in different layers with respect to ISO OSI layer in the table-1 [25].

Table 1
Layering-based attacks and possible security approach

Layer	Attacks	Security Approach
Physical Layer	Jamming and Tampering	Use spread-spectrum techniques and MAC layer admission control mechanisms
Data Link layer	Jamming and collision	Use error correcting codes and spread-spectrum techniques
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	injects false messages and energy drain attacks	Authentication
Application Layer	Attacks on reliability	Cryptographic approach

5 Secure Aggregation Schemes

The resource constrained sensor nodes and necessity of plain data for aggregation process pose great challenges when implementing security and data aggregation together. This section attempts to describe the secure data aggregation schemes.

- The first secure data aggregation (SDA) was proposed by Hu & Evans (2003) who studied the problem of data aggregation once one node is compromised. This protocol achieves resilience against a node compromise by delaying the aggregation and authentication at the upper levels. Therefore, sensors measurements are forwarded unchanged and then aggregated at the second hop instead of aggregating them at the immediate next hop.

Thus, the sensor needs to buffer the data to authenticate it once the shared key is revealed by the base station. Moreover, the proposed scheme only offers data integrity, freshness and authentication. Even though it increases the confidence in the sensor readings integrity the data can be altered once a parent and child in the hierarchy are compromised. Once a compromised node is detected, no practical action is taken to reduce the damage caused by this compromise which affects the data availability in the network. Much worse, once a grandfather node detects a node compromise, it could not decide whether the cheating node is the child or the grandchild.

- SDA scheme is improved in ESA by Jadia & Mathuria (2004). Instead of using μTESLA to authenticate the base station's broadcast in the validation process to reveal the shared key with sensors, the authors used one-hop pairwise keys (to encrypt data between a node and its parent) and two-hop pairwise keys (to encrypt data between a node and its grandparent). This will improve the secure aggregation scheme by adding data confidentiality and reducing the memory overhead since data does not need to be stored until the key is revealed.
- Przydatek et al. (2003) proposed a secure information aggregation (SIA) framework for WSNs called aggregate-commit-prove. This framework provides resistance against a special type of attack called stealthy attacks aggregate manipulation where the attacker's goal is to make the user accept false aggregation results without revealing its presence to the user. It consists of three node categories: a home server, a base station, and sensor nodes. SIA assumes that each sensor has a unique identifier and shares a separate secret cryptographic key with both the home server and the aggregator. The keys enable message authentication and encryption if data confidentiality is required. SIA consists of three parts: collecting data from sensors and locally computing the aggregation result, committing to the collected data, and reporting the aggregation result while proving the correctness of the result. SIA offers data integrity, authentication, data freshness, and confidentiality (if required). A witness based data aggregation (WDA) scheme for the WSN is being proposed by Du et al. (2003) to assure the validation of the data sent from an aggregator node to the base station. In order to prove the validity of the aggregated result, the aggregator node has to provide proofs from several witnesses. A witness is one who also performs data aggregation like the aggregator node, but does not forward its result to the base station. Instead, each witness computes the message authentication code (MAC) of the result and then sends it to the aggregator node which must forward the proofs to the base station.
- Moreover, SecureDAV (Mahimkar & Rappaport 2004) improved the data integrity vulnerability in SDA and ESA by signing the aggregated data. In SecureDAV, each sensor within a cluster will have its share of its secret cluster key and then it will be able to generate a partial signature on the aggregated data. Once an aggregator receives sensor readings in the same cluster, it aggregates them and broadcasts the average value of the readings. Each sensor in the cluster compares its reading with the average value received from the aggregator. Then, it partially signs the average value only and only if the difference between the received average value and its reading is less than a certain value (threshold). Then, the aggregator (cluster-head) combines partial signatures to form a full signature of the aggregated results and sends it to the base station.
- Yang et al. (2006) proposed a secure hop-by hop data aggregation protocol (SDAP) that can tolerate more than one compromised node. SDAP is based on two principles: divide-and-conquer and commit-and-attest. In order to reduce the damage caused by compromising an aggregator at a high level in the per-hop aggregation scheme, SDAP uses the divide-and-conquer principle to divide the network tree into multiple logical subtrees which increases the number of aggregators and reduces the number of nodes in each subtree. Consequently, the damage caused by compromising an aggregator of a subtree is reduced. The other principle, that is commit-and-attest, enhances the ordinary hop-by hop aggregation scheme by adding a commitment property, and helps the base station to prove the correctness of the aggregated data.

- Furthermore, Chan et al. (2006) extended the work in SIA by applying the aggregate-commit-prove framework in fully a distributed network instead of single aggregator model. In general, this scheme (SHDA) offers exactly what the SIA does data integrity, authentication, and confidentiality. Each parent sensor performs an aggregation function whenever it has heard from its child nodes. In addition, it has to create a commitment to the set of the input used to compute the aggregated result by using a merkle hash tree. Then, it forwards the aggregated data and the commitment to its parent until it reaches the base station. Once the base station received the final commitment values, it rebroadcasts them into the rest of the network in an authenticated broadcast. Each node is responsible for checking whether its contribution was added to the aggregated data or not.
- Sanli et al. (2004) developed a new data aggregation technique called the Secure Reference-Based Data Aggregation scheme (SRDA) that sends only the difference between sensed data and the reference value (called differential value) instead of raw data. Deference value is taken as the average value of previous sensor readings. In SRDA scheme, each sensor computes the differential data (sensed data - reference value), encrypts it, and then sends it to the cluster-head.
- Moreover, the problem of aggregating encrypted data in the WSN is being addressed in (Westhoff et al. 2006). The proposed protocol, called Concealed Data Aggregation (CDA), uses an additive and multiplicative homomorphic encryption scheme that allows the aggregator to aggregate encrypted data.
- Furthermore, a new secure data aggregation scheme based on homomorphic encryption (EDA) is proposed by (Castelluccia et al. 2005) This allows an aggregator to execute the aggregation function and aggregate the encrypted data that are received from its children with no need for decryption and to recover the original messages. It uses a modular addition instead of the xor (Exclusive-OR) operation that is found in the stream ciphers.

6 CONCLUSION

This paper provides a detailed review of secure data aggregation concept in wireless sensor networks. To give the motivation behind secure data aggregation, first, the security requirements of wireless sensor networks are presented and the threat model and adversarial model are explained to effectively handle security requirements of WSN. Second, an extensive literature survey is presented by summarizing the data aggregation protocols. There are still open issues with WSN security requirements which enforce security for duplicate sensitive aggregation functions during data aggregation process.

REFERENCES:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102– 114.

[2] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Networks 52 (12) (2008) 2292–2330.

[3] James Reserve Microclimate and Video Remote Sensing. http://www.cens.ucla.edu.

[4] Habitat Monitoring on Great Duck Island. http://www.greatduckisland.net/.

[5]The Firebug Project. http://firebug.sourceforge.net.

[6] K. Akkaya, M. Demirbas, R.S. Aygun, The Impact of Data Aggregation on the Performance of Wireless Sensor Networks, Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8 (2008) 171–193.

[7] L. Hu, D. Evans, Secure aggregation for wireless networks, in: Proceedings of the Workshop on Security and Assurance in Ad Hoc Networks, Orlando, FL, 28 January 2003.

[8] H. Çam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, H.O. Sanli, Energy-efficient and secure pattern based data aggregation for wireless sensor networks, Comput. Commun., Elsevier 29 (4) (2006) 446–455.

[9] Yoneki, E. & Bacon, J., (2005) "A survey of Wireless Sensor Network technologies: research trends and middleware's role", technical report. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.

[10] Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V., (2007) "Wireless sensor network security - a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC
Press.

[11] Fernandes, L. L., (2007) "Introduction to Wireless Sensor Networks Report", University of Trento.
http://dit.unitn.it/~fernand/downloads/iwsn.pdf

[12] Zia, T. A., (2008), "A Security Framework for Wireless Sensor Networks".
http://ses.library.usyd.edu.au/bitstream/2123/2258/4/
02whole.pdf

[13] Stallings, W., (2000) Cryptography and Network Security Principles and Practice, Cryptography Book, 2nd Edition, Prentice- Hall, 0-13-869017-0.
[14] Kaplantzis, S., (2006) "Security Models for Wireless Sensor Networks", http://members.iinet.com.au/~souvla/transferfinal-rev.pdf
[15] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., (2000) "Protocols for Self- Organization of a Wireless Sensor Network", IEEE Personal Communications, pp. 16-27.
[16] Woo, A. and Culler, D., (2001) "A Transmission Control Scheme for Media Access in Sensor Networks", Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy.
[17] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. & Chandrakasan, A., (2001) "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", Proceedings of the 7th Annual
International Conference on Mobile Computing and Networking, Rome, Italy, pp. 272-287.
[18] Shen, C., Srisatjapornphat, C., and Jaikaeo, C., (2001) "Sensor Information Networking Architecture and Applications", IEEE Pers. Communication, pp. 52–59.
[19] Committee on National Security Systems (CNSS), (2006) National Information Assurance Glossary, NSTISSI,No. 4009.
[20] Wood, A. and Stankovic, J. A., (2002) "Denial of Service in Sensor Networks", IEEE Computer, 35(10):54-62, pp. 54-62.
[21] Fernandes, L. L., (2007) "Introduction to Wireless Sensor Networks Report", University of Trento.
http://dit.unitn.it/~fernand/downloads/iwsn.pdf
[22] Siahaan, I. and Fernandes, L. (2008), "Secure Routing in Wireless Sensor Networks", University of Trento.
http://dit.unitn.it/~fernand/downloads/IWSNSlides.pdf
[23] Dimitrievski, A., Stojkoska,B, Trivodaliev, K. and Davcev, D., (2006) "Securing communication in WSN trough use of cryptography", NATO-ARW, Suceava.
[24] Parno, B., Perrig, A. and Gligor V., (2005) "Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of the IEEE Symposium on Security and Privacy (S&P'05).
[25] Saxena, M., (2007) "Security in Wireless Sensor Networks – A Layer based classification", Technical Report [CERIAS TR 2007-04], Center for Education and Research in Information Assurance and Security - CERIAS, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04- cerias.pdf

Priyanka K. Shah has completed her Bachelor of Computer Applications from Gujarat University in 2005. In 2008, she holds distinction in the Master of Computer Application from Gujarat University. Since 2008, she is working with Charotar Institute of Computer Application, under Charotar University of Science and Technology, situated at Changa, as an Assistant Professor. She is pursuing Ph.D. in the subject of Wireless Sensor Networks.

Kajal V. Shukla has completed her Bachelor of Science from Gujarat University in 2005. In 2008, she holds degree of Master of Computer Application from Gujarat University, Since 2008, she is working with Charotar Institute of Computer Application, under Charotar University of Science and Technology, situated at Changa, as an Assistant Professor. Currently she is working in the area of Wireless Networks.