# A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks

Kalpana Sharma[1], M.K. Ghose[1], Deepak Kumar[1],
Raja Peeyush Kumar Singh[1], Vikas Kumar Pandey[1]
[1]*CSE, Sikkim Manipal Institute of Technology*
*kalpanaiitkgp@yahoo.com, mkghose@smu.edu.in, deepakkumar.ce@gmail.com, rajapeeyushkumarsingh200611081@yahoo.com,vikas200611130@gmail.com*

***Abstract***

*The security in wireless sensor networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage. While a variety of security techniques are being developed and a lot of research is going on in security field at a brisk pace but the field lacks a common integrated platform which provides a comprehensive comparison of the seemingly unconnected but linked issues. In this paper we attempt to comparatively analyse the various available security approaches highlighting their advantages and weaknesses. This will surely ease the implementers' burden of choosing between various available modes of defence.*

**Keywords:** WSN, DoS, Security, Cross layer.

## 1. Introduction

Wireless sensor networks (WSN's) are quite useful in many applications since they provide a cost effective solution to many real life problems. But it appears that they are more prone to attacks than wired networks .They are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service, prompting a range of fundamental research challenges [1], an attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes. Security allows WSNs to be used with confidence and maintains integrity of data. Without security, the use of WSN is any application domain would result in undesirable consequences. Particularly in military based projects where a compromise in security can lead to disastrous consequences. Thus security must be addressed in such critical sensor applications. It turns out that providing security in wireless sensor networks is pivotal due to the fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation, and storage. Efficiency is thus a crucial issue, as sensors are usually deployed in remote area for a long time. Although a lot of progress has been made for the past few years, the field remains fragmented, with contributions scattered over seemingly disjoint yet actually connected areas. As for example key management only makes sure the communicating nodes possess the necessary keys, at the same time protecting the confidentiality, integrity and authenticity of the communicated data. However it only assures a sense of security in one layer whereas the security of the network can be ruptured in other layers as well like network layer, physical layer etc.

In this paper we explore various security issues in wireless sensor networks and try to give a comparative note of various existing security approaches. Our contribution is therefore to provide a detailed yet concise analysis of various existing techniques which will enable the WSN implementers to approach security in an organised way.

The rest of this paper is organized as follows. Section 2 lays down the principles in view of which our analysis is built. Section 3 describes various types of threats and attacks and preferable mode of defence. Section 4 concludes.

## 2. Issues in WSN security

Security mechanisms in WSN are developed in view of certain constraints. Among these, some are pre-defined security strategies; whereas some are direct consequences of the hardware limitations of sensor nodes. Some of the issues described here pave way for the guidelines in the next section:

1) Energy efficiency: The requirement for energy efficiency suggests that in most cases computation is favoured over communication, as communication is three orders of magnitude more expensive than computation [5]. The requirement also suggests that security should never be overdone - on the contrary, tolerance is generally preferred to overaggressive prevention [2]. More computationally intensive algorithms can not be used to incorporate security due to energy considerations.

2) No public-key cryptography: Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy [3]. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-key-cryptography is very much viable for smaller networks [5].

3) Physically tamperable: Since sensor nodes are low-cost hardware that are not built with tamper-resistance in mind, their strength has to lie in their number. Even if a few nodes go down, the network survives. The network should instead be resilient to attacks. The concept of resilience, or equivalently, redundancy-based defence is widely demonstrated [2, 4, 1].

4) Multiple layers of defence: Security becomes an important concern because attacks can occur on different layers of a networking stack (as defined in the Open System Interconnect model). Naturally it is evident that a multiple layer of defence is required, i.e. a separate defence for each layer [2]. The issues mentioned here are in general applicable to almost all sorts of domain irrespective of their traits.

### 2.1 Security requirements

**2.1.1 Availability:** Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale wireless sensor networks. A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network [37]. Moreover, wireless sensor networks are vulnerable to various attacks. The adversary is assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors. Equipped with richer resources, the adversary can launch even more serious attacks such as DoS attack, resource consumption attack and node compromise attack.

**2.1.2 Confidentiality:** Data confidentiality is the most important issue in network security. Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties can not read information between two communicating parties. A sensor network should not leak sensor readings to its

neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive [37].

• In many applications, nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Generally, encryption is the most widely used mechanism to provide confidentiality.

**2.1.3 Integrity and authenticity:** Confidentiality only ensures that data can not be read by the third party, but it does not guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor networks use wireless broadcasting as communication method. Thus it is more vulnerable to eavesdropping and message alteration [1]. Measures for protecting integrity are needed to detect message alteration and to reject injected message. Authentication ensures that the sender was entitled to create the message and that the contents of the message have not been altered. In the public key cryptography, digital signatures are used to seal a message as a means of authentication. In the symmetric key cryptography, MACs are used to provide authentication. When the receiver gets a message with a verified MAC, it is ensured that the message is from an original sender. Digital signature is based on asymmetric key cryptography (e.g., RSA), which involves much more computation overhead in signing/decrypting and verifying/encrypting operations. It is less resilient against DoS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim's computation resources for verifying them [2].

**2.1.4 Data freshness:** Data freshness means that the data is recent and any old data has not been replayed. Data freshness criteria are a must in case of shared- key cryptography where the key needs to be refreshed over a period of time. An attacker may replay an old message to compromise the key.

**2.1.5 Self organisation:** Due to the ad-hoc nature of WSNs it should be flexible, resilient, adaptive and corrective in regards to security measures.

## 3. Various types of threats & attacks in different layers & preferable modes of defence

Security attacks in sensor networks can be broadly classified into Passive attacks and Active attacks. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The motive of the attacker is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. Basically we are mainly looking .at two types of protection: protection from denial-of-service (DoS) attacks, and protection of the secrecy of information. Multiple defences, each for one layer of the networking stack should be implemented. One layer is discussed at a time:

### 3.1. Physical Layer

The Physical layer refers to mechanical, electrical, functional and procedural characteristics to establish, maintain and release physical connections (e.g. data circuits, radio interfaces) between data link entities. This layer defines certain physical characteristics of the network, for example the frequency, the data rate, the signal

modulation and the spread spectrum scheme to use. DoS attacks on the physical layer are radio jamming. Well-known countermeasures to radio jamming include adaptive antenna systems, spread spectrum modulations, error correcting codes and cryptography. There is not much room to manipulate in antenna systems and error correcting codes because sensor nodes typically use an omnidirectional antenna and Reed-Solomon codes [9-12]. We mainly focus on spread spectrum modulations in this section, and will talk about cryptography in Section 3.5 .Ideally the transceiver should support some form of spread spectrum modulation, preferably frequency-hopping spread spectrum (FHSS), instead of direct-sequence spread spectrum (DSSS). FHSS is preferred to DSSS, because DSSS requires more circuitry (higher cost) to implement, is more energy consuming and more sensitive to environmental effects [14,15]; on the other hand, the hop rate in a FHSS system is typically much lower than the chip rate in a DSSS system, resulting in lower energy usage [14, 16].

However a unique DSSS modulation method is described and evaluated that enables a high data rate, which is desirable to minimize total transceiver active time and, therefore, maximize battery life, while minimizing transceiver complexity [38].

### 3.2. Data Link Layer

The data link layer defines how data are encoded and decoded, how errors are detected and corrected, the addressing scheme as well as the medium access scheme.

According to results in link-layer jamming [6, 7], smart jammers can take advantage of the data link layer to achieve energy-efficient jamming. In the earlier work [6],it was shown that S-MAC can be jammed energy-efficiently by jamming the control interval of the listen interval alone [6], so we recommend encrypting packets on the data link layer, for example as done in TinySec [8]. An elaborate encryption scheme depends on the key management architecture which will be discussed in Section 3.5. In the latter work [8], it was shown that even when the packets are encrypted, the temporal arrangement of the packets induced by the nature of the protocol exposes patterns that the jammer can exploit. Thus link-layer jamming is more energy efficient for the attackers as compared to radio-jamming in physical layer.

TDMA protocols like LMAC [19] have better anti-jam properties, and therefore should be preferred to other protocols like S-MAC [20, 21] and B-MAC [22].

### 3.3. Network Layer

The International Standards Organization (ISO) model for Open Systems Interconnection (OSI) states that the network layer "provides functional and procedural means to exchange network service data units between two transport entities over a network connection depending upon parameters such as latency or energy. It provides transport entities with independence from routing and switching considerations."

There are 2 types of routing protocols for WSNs: (1) ID-based protocols, in which packets are routed to the destination designated by the ID specified in the packets themselves; and (2) data-centric protocols [17] , in which packets contain attributes that specify what kinds of data are being requested or provided. The discussion considers any action that results in any combination of the following an attack [18]:

**3.3.1. Neglect**: Packets are dropped or discarded completely, or selectively forwarded by an anonymous party.

**3.3.2. Flooding**: The network is flooded with global suspicious broadcasts.

**3.3.3. Misdirection/Homing:** Some sensor nodes in the network are misguided into believing that nodes that either are multiple hops away, or that do not exist at all are their neighbours. This is called a **Sybil attack**.

**3.3.4. Wormholes:** A considerable amount of the network traffic is tunnelled from one place in the network to another distant place of the network, depriving other parts of the network that under normal circumstances would have received the traffic themselves. This is called a **wormhole attack.** This tunnelling or retransmitting of bits can be done selectively.

**3.3.5. Blackholes:** In flooding based protocols, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Thus it attracts a large portion of traffic and acts as a blackhole for the network. This is called a **sinkhole or blackhole attack**. This attack can be facilitated by the wormhole attack.

**3.3.6. Looping:** Some routes form loops or detours. These attacks are sophisticated forms of DoS attacks.

Among these attacks, we ignore the last one because we do not see any significant value for the attackers in it - causing loops is not more efficient than just dropping or discarding packets; causing detours is an inefficient way of wasting the sensor nodes' energy.

-The first attack is countered using multipath routing [13].

-The second attack is countered using authenticated broadcasts, which has to be facilitated by the underlying key management architecture.

-Sybil, wormhole and sinkhole attacks require the attackers to manipulate packets. To prevent this, key management architecture is required. In particular, Sybil attacks can be countered using random key pre-distribution schemes, to be discussed in Section 3.5.

-Against wormhole attacks and hence sinkhole attacks, so far there is no resource-lean and energy-efficient countermeasure, i.e. with or without key management, wormhole and sinkhole attacks are still an open issue.

In [40] the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defence mechanism for preventing jamming DoS attacks.

We now describe our recommendation. Consistent with Karlof et al.'s analysis [23], we recommend using data centric protocols such as multipath directed diffusion[13] , or geographic routing protocols [24,25] in case the nodes are able to determine their own locations, because these protocols include flooding as a robust way of disseminating information. The security of geographic routing protocols depends on the correctness of the location information, as such secure geographic routing requires secure localization, as described in [43]. In conjunction with these protocols, the data link layer should support encryption and authentication, just as we have recommended in the previous section, whereas the key management architecture should support authenticated broadcasts and random key pre-distribution. In general, the above strategy is not effective against wormhole and sinkhole attacks but the data link layer is easier to DoS attack than the network layer, so if the security of the network is somewhat relaxed, then data link layer should at least be made as resistant to DoS attacks as possible. In case we need to use ID-based routing, it is recommended to use endairA [26], an improved version of Ariadne [27], because it is provably more secure against an attacker with a single compromised key and a single compromised node. However, it does not support multipath routing. Furthermore, the corresponding key management architecture has to support node-specific key pre-distribution (i.e. every node has to share one key with every other node in the network), in addition to authenticated broadcasts.

### 3.4. Application Layer

The application layer refers to the topmost layer of the protocol stack. It is responsible for managing / processing (aggregation of data etc.) the data and verifying its correctness. In WSN, data aggregation is a vital primitive enabling efficient data queries. An on-site aggregator device collects data from sensor nodes and produces an aggregate gist of data which is sent to the off-site querier, thus reducing the communication cost of the query. It is common for data to be aggregated, for example, the temperature readings of a particular region of the network to be averaged. However averaging is not a secure aggregation function [28]. A better solution is to use the median of the data. An aggregation function should qualify for resistance to attacks using Wagner's technique [28]. However it is noteworthy that Wagner's result is only applicable if the aggregator node is in range with all the source nodes, that is if there's no other intervening aggregator between the aggregator and the source nodes. This scheme is applicable to cluster-based networks where a cluster head can act as an aggregator for its cluster members.

To guarantee that if the home server accepts an aggregation result from the aggregator, the reported result is close to the true aggregation value with high probability, Przydatek et al. [28] propose a communication-efficient transaction paradigm called aggregate-commit-prove, which in effect provides two layers of defence against data corruption. The first defence is commitment (hence the word 'commit' in aggregate-commit-prove): the aggregator commits to the aggregated data, by cryptographic means. The second defence is interactive proofs (hence the word ‘proves'): the aggregator proves to the base station the validity of the aggregation result, by statistical means. The aggregator and home server need to share a key with each of the source nodes. Lazos et al.'s secure localization scheme [28] works on the assumptions that (1) the locators, i.e. the devices that provide trusted location information to other nodes, are tamper-resistant, and (2) the density of locators is known to every node.

### 3.5. Cross-Layer

Though a number of approaches have been proposed to provide security solutions against various threats to the WSN based upon the layered design. These layered approaches are often inadequate and inefficient, and it is advantageous to break with the conventional layering rules and design the security scheme for the WSN based on information from several protocol layers. There are two cross-layer services that are of concern: (1) *key management,* and (2) *intrusion detection* and response.

**3.5.1. Key managemen**t: It is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, refreshed and destroyed.

The key management scheme we are recommending is based on Zhu et al.'s LEAP [29], extended according to our earlier analysis of the data link layer, the network layer and the application layer. Before giving the details, it is useful to discuss an important concept of LEAP: passive participation [44]. In passive participation, a node that overhears its neighbour’s transmitted data may choose not to transmit its data if its neighbour’s data are the same as its own data, thereby saving energy. To exhibit passive participation, a node has to share a key, called by Zhu et al [29] the cluster key, with its neighbours. The node also has to establish a one-way key chain [30] and send the commitment of the key chain to its neighbours to allow its neighbours to authenticate its locally broadcast messages. The combination of a cluster key and a one-way key chain is necessary because [43]:

- if only the cluster key is used, a compromised neighbour would disclose the cluster key.
-if only the key chain is used, the keys in the key chain would have to be broadcast, allowing replay attacks to take place.

- but if used together they complement each other, the cluster key can be used to hide the keys in the key chain from cluster-outsiders, so that the keys do not need to be disclosed according to a schedule as in SPINS, and the keys in the key chain can be used for authentication as usual.

We now present the details. The network can be bootstrapped, and nodes can be added /removed following the protocols of LEAP [29]. We deduce [43] the following keys are needed on each sensor node (for ease of discussion, we give the role of sink nodes / aggregators / locators to the base stations):

- For link-layer encryption and authentication, 1 network-wide key.
- For authenticated broadcasts, b commitments of b one way key chains, where b is the number of base stations that can broadcast globally.
-If the routing protocol is a data-centric protocol and the network is static, d pair wise keys that are shared with the node's d neighbours.
-If the routing protocol is a data-centric protocol and the network is mobile, a fixed number k of randomly pre-distributed keys.

Note: These d pairwise keys or k randomly pre-distributed keys are for countering Sybil attacks. Using k randomly pre-distributed keys allows a node to be mobile and yet establish secure connections with new neighbours, although with reduced connectivity.

- If the routing protocol is endairA (the only ID-based routing protocol we recommend), n- 1 keys where n is the total number of nodes in the network.
- For Przydatek et al.'s secure information aggregation [28] (as discussed in the previous section), 1 shared key with the base station and 1 shared key with the home server if the node is a source node.
-For passive participation, d + 1 cluster keys, d commitments of the one-way key chains of its neighbours, 1 one-way key chain of itself, where d is the number of neighbours.

One-way chains [45] are an important cryptographic primitive in building an energy-efficient key-management scheme. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature [45].

**3.5.2. Intrusion detection:** Intrusion detection and response is the process of monitoring anomalies on the network, detecting the invasion of any outsider node (adversary) and verifying whether anomalies are a result of intrusions and responding with appropriate countermeasures.

The existing secure protocols or intrusion detection schemes are normally proposed for one protocol layer. What should be classified as an anomaly is totally application-specific. A sensor node can recognize some anomalies as intrusions on its own, e.g. whether it is jammed (Section 3.1), but for some other anomalies like whether it is being targeted with Sybil attacks (misinformed identity), it needs to communicate with its neighbours (Section 3.3). But there are chances that even some of its neighbours themselves may be intruder, several reputation-based schemes have been proposed [33-36]. In these schemes, a node rates the reputation of a. neighbour based on whether the neighbour is 'cooperative'. A node's ability to evaluate cooperativeness is however questionable. For example, merely receiving data from its neighbour does not imply that the neighbour is cooperating if the data is false. But how to verify that this data is false or not. The node may consult other neighbours on the validity of the data, but depending on what value is measured, the other neighbours may or may not be able to corroborate the data's validity. However this approach is energy consuming, its better to assign the job of validating data to a secure aggregator (Section 3.4).We do not see reputation-based schemes as playing an essential role in the security of WSNs. Different intrusion responses are applicable to different layers, and are already discussed in the respective layers.

The following table summarizes the various types of attacks in each layer, possible modes of defence, best/optimal approach and priority that should be given for the security of each layer.

**Table 1:** The table shows possible attacks and modes of defence in each layer and the priority* for security concern in each layer w.r.t other layers.

| Layer | Main security concern | Available Modes of defence | | | Best/optimal choice | Prior-ity* |
|---|---|---|---|---|---|---|
| | | Mode | Strength | Weakness | | |
| Physical layer | -DoS attacks like radio jamming | DSSS | -high data rate<br>-less transceiver-active time | -more circuit<br>- more energy reqd.<br>-affected by environmental factors<br>-high chip rate | FHSS with 500-1000 hops/sec using FSK(frequency-shift-keying) | 4 |
| | | FHSS | -less energy reqd.<br>-lower hope rate | -difficult for ND &association<br>-larger warm-up period | | |
| | -Physical tampering | | | | Tamper-resistant Hardware /Hiding | |
| Data link layer | -Sleep deprivation-torture attacks[39]<br>-Listen-interval jamming<br>-CTRL Interval jamming[6] | ALOHA | -good for low throughput & low SNR systems | -less battery life<br>-not fit for multi-hop networks | Distributed MD protocol OR TDMA | 1 |
| | | CSMA | -high duty-cycle | -frequent active periods<br>-hidden node problem<br>-needs synchronization | | |
| | | Distributed MD(mediation device) protocol | -low cost<br>-good battery life<br>-dynamic synchronization | | | |
| | | TDMA | -logical channel reservations | -poor battery life | | |
| | | POLLING | Good for low-latency networks | -difficult to achi | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | eve low duty - cycl e | | |
| | Collision | S-MAC | -low energy -low overhead Idle listening | Pron e to CTR L jam min g | Error Correcting Code | |
| | | Error correcting code | | | | |
| | Data packet jamming | Encryption | -Integrity, -confidentiality -authenticity | Com puta tion al cost | Data blurting Or schedule Switching[6] | |
| Networ k layer | Neglect/ discard | | | | Multipath routing | 2 |
| | Hello-Flooding | | | | Authenticated Broadcast & Efficient Key-management | |
| | Blackholes | Key Management Schemes | | | REWARD algorithm[41] | |
| | Sybil | -Radio-resource testing -random key Predistribu-tion | | | Key-management Architecture | |
| | Wormholes | TIK | Implements Temporal - leashes | - Req uires sync hron izati on - com puta tion ally expe nsiv e | TIK[42] based upon symmetric cryptography | |
| Applica -tion layer | Aggregation-based attacks | | | | Aggregate-commit-prove framework[28] | 3 |

## 4. Conclusion

WSN security is a very important issue which is motivated towards ensuring security under the strict constraints of computational power, energy and other hardware constraints. Furthermore, the following points can be added. Security of a WSN is dependent on securing all the layers.

We firstly discussed security, addressing all the layers individually and then discussed the cross-layer approach which is needed to tackle some sophisticated attacks. However

an integrated approach of secured routing protocol and key-management architecture would definitely yield a better security measure. Until then, our survey should serve the purpose of a first-hand guideline on establishing a secured WSN.

## 5. References

[1]Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53{57, 2004.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[3] D. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.[Online]. Available: http://download.nai.com/products/media/pgp/pdf/sensit-workshop- 100799.pdf

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[5] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.

[6] Y. Law, P. Hartel, J. den Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC," in 2nd European Workshop on Wireless Sensor Networks (EWSN 2005). IEEE, 2005, pp. 217-225. [Online]. Available: http://ieeexplore.ieee.orgliel5/9875/3139l/01462013.pdf

[7] Y. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols," in The Third ACM Workshop oni Security of Ad Hoc and Sensor Networks (SASN 2005). ACM Press, 2005, to appear.

[8] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 2004, pp. 162-175.

[9] G. Lin and G. Noubir, "Low Power DOS Attacks in Data Wireless LANs and Countermeasures," Northeastern University, Tech. Rep., 2002. [Online]. Available: http://www.ccs.neu.edu/home/noubir/publications/LN02a.pdf

[10] , "On Link Layer Denial of Service in DATA Wireless LANs,"Wiley Journal on Wireless Communications and Mobile Computing,To appear. [Online]. Available: http:llwww.ccs.neu.edu/home/noubir/publications/LN05.pdf

[11] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-30, 2003.

[12] D. C. Schleher, Electronic Warfare in the Information Age. Artech

[13] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly resilient, energy efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review (MC2R), vol. 1, no. 2, 2002.

[14] J. Min, "Analysis and design of a frequency-hopped spread-spectrum transceiver for wireless personal communications," Ph.D. dissertation, University of California, Los Angeles, 1995. [Online]. Available: http://www.icsl.ucla.edu/aagroup/PDF-files/tcvr-arch.pdf

[15] G. J. Pottie and L. P. Clare, "Wireless integrated network sensors: toward low-cost and robust self-organizing security networks," in Sensors, C31, Information, and Training Technologies for Law Enforcement, ser. SPIE Proceedings, vol. 3577, 1999, pp. 86-95. [Online]. Available: http://wins.rsc.rockwell.comlpublications/spie3577- 12.pdf

[16] K. Tovmark, Chipcon Application Note AN014: Frequency Hopping Systems (Rev. 1.0), Chipcon AS, Mar. 2002. [Online]. Available: http: //www.chipcon.com/files/AN-014-Frequency..hopping-Systems-1-0.pdf House, July 1999.

[17] D. Ganesan, A. Cerpa, Y. Yu, and D. Estrin, "Networking issues in wireless sensor networks," Journal of Parallel and

Distributed Computing (JPDC), Special issue on Frontiers in Distributed Sensor Networks, To appear. [Online]. Available: http://lecs.cs.ucla.edu/-deepak/PAPERS/jpdc.pdf

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, pp. 293-315, 2003. [Online]. Available: http://www.cs.berkeley.edu/-daw/papers/

[19] L. van Hoesel and P. Havinga, "A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks: Reducing Preamble Transmissions and Transceiver State Switches," in INSS, June 2004.

[20] W. Ye, J. Heidemann, and D. Estrin, "An Energy-Efficient MAC protocol for Wireless Sensor Networks," in Proc. IEEE Infocom, USC/Information Sciences Institute. New York, NY, USA: IEEE, June 2002, pp. 1567-1576. [Online]. Available: http://www.isi.edu/johnh/PAPERS/Ye02a.html

[21] , "Medium Access Control with Coordinated, Adaptive Sleeping for Wireless Sensor Networks," IEEE/ACM Transactions on Networking, vol. 12, no. 3, pp. 493-506, 2003. [Online]. Available: http: //ieeexplore.ieee.org/iel5/90/29000/01306496.pdf

[22] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM Press, 2004, pp. 95-107.

[23]C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, pp. 293-315, 2003. [Online]. Available: http://www.cs.berkeley.edu/-daw/papers/

[24] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003.

[25] , "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Performance," IEEE Transaction’s on Mobile Computing, vol. 2, no. 4, pp. 349-365, 2003.

[26] L. Buttyan and I. Vajda, "Towards provable security for ad hoc routing protocols," in SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM Press, 2004, pp. 94-105.

[27] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in Proc. 8th Annual Ilt. Colf on Mobile Computing and Networking. ACM Press, 2002, pp. 12-23.

[28]B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in Proceedings of the 1st international conference oni Embedded networked sensor systems. ACM Press, 2003, pp. 255-265.

[29] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in 10th ACM Conference on Computer and Communications Security (CCS '03). ACM Press, 2003, pp. 62-72.

[30] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," in Proceedings of the 7th Ann. Int. Conf on Mobile Computing and Networking. ACM Press, 2001, pp. 189-199.

[31]B. Preneel, "Cryptographic primitives for information authentication - state of the art," in State of the Art in Applied Cryptography, ser. LNCS, B. Preneel and V. Rijmen, Eds., vol. 1528. Springer-Verlag, 1998, pp. 50-105.

[32] S. Crosby and D. Wallach, "Denial of service via algorithmic complexity attacks," in 12th USENIX Security Symposium. USENIX Association, 2003, pp. 29-44. [Online]. Available: http:H/www.cs.rice.edu/scrosby/hash/CrosbyWallach-UsenixSec2003/index.html

[33] P. Michiardi and R. Molva. "Core: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," in Communications and Mtultimedia Security Conference, 2002. [Online]. Available: http://www.eurecom.fr/-michiard/pub/michiardi-adhoc-core.Ps

[34] , "Prevention of denial of service attacks and selfishness in mobile ad hoc networks,' Institut Eurecom, France, Research Report RR-02- 063, 2002. [Online]. Available: http://www.eurecom.fr/-michiard/pub/ichiardi_adhoc_dos.ps

[35] , "Simulation-based analysis of security exposures in mobile ad hoc networks," in European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, Febrntary 25-28, 2002, Florence, Italy, 2002.

[36] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM Press, 2004, pp. 66-77.

[37] Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. 2006 Auerbach Publications, CRC Press

[38] Wireless sensor networks-Architecture and protocols-CRC press

[39] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Proceedings of The 7th International Workshop on Security Protocols*, volume 1796 of *LNCS*, pages 172–194. Springer- Verlag, 2000.

[40] Younis, M., Youssef, M., and Arisha, K., “Energy-aware routing in cluster-based sensor networks” Proc. 10th IEEE International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.

[41] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

[42]Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986

[43]N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *ACM Workshop on Wireless Security*, September 2003.

[44]How to Secure a Wireless Sensor Network Yee Wei Law Paul J.M. Havinga- IEEE 2005

[45] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes. PGP in constrained wireless devices. In *Proceedings of the 9th USENIX Security Symposium*, pages 247–261. USENIX, August 2000

## Authors

**Kalpana Sharama** , B.tech , M.tech
(IIT,Kharagpur)
Reader, CSE, SMIT
Area of Specialisation:- Wireless sensor network and Security.

**Dr. M.K.Ghose** is the Professor and Head of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Majitar, Sikkim, India. Prior to this, Dr. Ghose worked in the internationally reputed R & D organisation ISRO – during 1981 to 1994 at Vikram Sarabhai Space Centre, ISRO, Trivandrum in the areas of Mission simulation and Quality & Reliability Analysis of ISRO Launch vehicles and Satellite systems and during 1995 to 2006 at Regional Remote Sensing Service Centre, ISRO, IIT Campus, Kharagpur in the areas of RS & GIS techniques for the natural

**Deepak Kumar**
Final Year student, CSE, SMIT
Area of Interest: - Security implementation in WSN using LFSR and real time data capturing using GPS for WSN.

**Raja Peeyush Kumar Singh**
Final Year student, CSE, SMIT
Area of Interest: - Security implementation in WSN using LFSR and real time data capturing using GPS for WSN

**Vikas Kumar Pandey**
Final Year student, CSE, SMIT
Area of Interest: - Security implementation in WSN using LFSR and real time data capturing using GPS for WSN