A Study on the Security Issues in WSN

Tasneem Halim
Department of Computer Science
Central Women's University (CWU)
6 Hatkhola Road, Dhaka – 1203m Bangladesh

Md. Rafiqul Islam
Department of Computer Science
American International University-Bangladesh
Dhaka, Bangladesh

ABSTRACT
Wireless Sensor Network has opened several research criteria related to social security, data management, networking models, distributed system, agricultural aspects, military supervision etc. With the increasing number of applications, an increment in sensor network vulnerabilities has also become noticeably higher. For numerous purposes along with tracing and tracking objects, the sensor nodes with limited power supply, memory usage and computation capability are used to collect data, process it and transmit the generated results to other sensing devices over a specific geographic area. This whole process is done using wireless communication channels which are susceptible to various security threats. Thus securing the WSN has become a great challenge for the researchers. The objective of this paper is to explore these security issues and challenges regarding WSN by classifying security attacks, reviewing proposed security mechanisms and clarifying essential security requirements for specific security schemes. Finally, the relativity between proposed solutions against specific security threats of WSN is shown in a tabular form.

General Terms
Wireless Sensor Network Security, WSN security

Keywords
WSN, Vulnerabilities, Sensor network, Security, Attack, Challenge, Threat

1. INTRODUCTION
Wireless Sensor Network (WSN) is an advanced heterogeneous technology which includes large-scale sensing technology combined with wireless communication, less processing power and limited energy consumption. It has opened several research criteria related to social security, data management, system design, programming and networking models, distributed system, agricultural aspects and military supervision etc [1], [2]. The main characteristics of WSN are less processing power with lower radio frequency, wireless techniques allowing less energy consumption and tiny sensor networks with the capability of sensing various different type parameters depending on sound, temperature, pollutant, pressure, motion, vibration etc from diverse locality [4]. For different numerous purposes like monitoring environment, defense security, surveillance, even for tracing and tracking, the sensor nodes with limited communication and computation capabilities collect data, store and/or process it and then transmit it to other sensing devices including base stations over a specific geographic area. These data may contain results after monitoring temperature, soil make-up, lighting condition, noise level, absence or presence of certain substances, stress level of machines attached with different objects etc [5]. A WSN containing hundreds of inexpensive sensors and sink nodes has to work in an inaccessible unsupervised atmosphere where its best performance is very much expected and a flawless transmission of data packet is required. Each node acts as a "source" or "destination" while communicating with each other through the wireless medium. So any interruption in transmission or failure of a node or even an intrusion attack in the network may cause huge damage. That is why the security of the WSN and its data are still a great challenge for the researchers [7]. However, the necessity to design any security scheme for WSN relies on a variety of causes; like:

The physical particles themselves are immensely vulnerable due to their hostile localization, less power supply, flexible infrastructure, temper resistant hardware and targeted cost reduction quality. Thus preventing corruption of sensor nodes is a great challenge before the execution of entire-network failure.

The wireless communication channels are more susceptible to various types of attacks specially eavesdrop ones. Moreover majority used protocols are publicly known due to their standardization which adds extra advantages in intrusive acts. Thus securing the transmission channels are extremely essential.

Moreover, restrictions in computation, memory usage and energy supply make the asymmetric cryptography more inappropriate for any WSN. Public-key cryptography could have been a better option due to its versatility but it complicates the design unexpectedly. Thus efficient symmetric cryptography is considered as the appreciated alternative.

Considering all these aspects, in this paper we took an effort to discuss the various security issues existing in WSN, like necessary security goals while designing a security schemes in section 2, available security threats and attacks often encounter in a WSN in section 3, proposed different types of security schemes and solutions for different types of attacks in section 4 and finally a summary of all these threats and solution as a conclusion in section 5.

2. SECURITY ISSUES IN WSN
The wireless communication technique used in a WSN often welcomes eavesdropping and intrusive code injection while transmitting data packets. Moreover, the randomly movable sensors with little energy consumption feature give the intruders numerous scopes to do DOS (Denial of Service) attack or MITM (Man-in-the-Middle) Attack which eventually reduces the security of the WSN. So a minimum security requirements and properties are expected to be achieved from any wireless sensor network [3]. To do so required security goals for any WSN are briefly described below.

2.1 Necessary security goals
Availability: Availability is a must required key concern to ensure the longevity of the WSN. In majority cases failure to

ensure the availability of the sensor nodes in a WSN causes Denial-of-service attacks which eventually lead to a massive loss in detecting potential data and financial crisis [7].

Authenticity: Since these networks use wireless channels to convey valuable data and information either processed or need to be processed, authentication of these transmitted data is equally important [6]. However, verification of the origin of the data or source authentication may prevent outdoor attacks but still some of the security problems remain unsolved.

Confidentiality: Confidentiality of the sensed data is essential to prevent malicious code insertion and spoofed packet detection [8]. It assures the transmitted data protection. And application of shared encryption key between the communicating nodes can be sufficient for that. However, an intruder may analyze the network traffic or use any decryption method to break into the network. So limitations in the access control right at the base stations are always suggested.

Data Freshness: It is also mandatory that all the received information is fresh and up-to-date; which means, no repetition of old records and an assurance of most recent data is collected [3]. To do that, each shared secret key is checked and guaranteed not to be reused by any other participant in the same network.

Flexibility: The sensor nodes in a wireless sensor network functions in critical environments where the condition, tasks, position of the nodes even the threats may change very frequently. Any of the sensor nodes may fuse down or being removed from the network. Again new nodes may be added into the network or a large network may split into small sensor networks depending on the situation. So the designed security scheme should be flexible enough to adjust and operate in any possible condition may encounter at any time [20].

Integrity: One of the most important services of wireless sensor network is data aggregation. In data aggregation, the sensor node collects readings from neighboring nodes, aggregates them, and sends them to the base station to process the data [9]. While this procedure goes on, data integration guarantees that the collected readings are original and not tampered or changed due to any reason.

Scalability: The dynamic environmental condition, number of sensor nodes in a WSN, magnitude of the nodes, even the topology of the sensor network keeps changing very frequently to allow insertion of new fresh nodes and deletion of fused nodes in a network [17]. However, an extension or reduction of the sensor network or replacement of any unreliable physical objects should not affect the performance of the WSN. That is why scalability in the security solution is mandatory.

Self-organizing Quality: A wireless sensor network is expected to be self-organized than deterministic. The designed solutions must adapt this quality as the normal scenario is the neighbor sensor in and WSN will not know its correspondent node in advance and the number of sensors, sink nodes, distance between the nodes, required power consumption, even the rate of data transmission will be not be defined in advance [9]. This requires the flexibility and assures the security of the sensor network.

3. DIFFERENT ATTACKS IN WSN

Wireless networks are generally more susceptible to numerous types of security threats due to the use of shared unreliable transmission medium. Any unguided transmission medium is more vulnerable to security threats than well-guided transmission medium. Either it is a wireless ad hoc network or wireless sensor network it is easily exposed to the intruders because of its broadcasting nature. In majority cases like military inspection, environment monitoring, motion detection etc, these tiny sensor nodes have to be deployed arbitrarily in hazardous situations. Thus defending these particles from security attacks has become a great challenge.

In this section, various security attacks in wireless sensor networks are explained. The major two divisions of WSN attacks are outsider attack and insider attack; in other sense attacks against basic routing mechanisms and attacks against security mechanisms [9], [13].

3.1 Denial – of – Service Attack:

Denial-of-Service attack in wireless sensor network occurs due to intentional intrusion attack or unexpected node failure [15], [16].Various software bugs, unexpected sensor node failure, exhausted power supply system, environmental disaster, complication in data transmission and communication or even intentional intruder attack may execute DoS attack. Often the outsiders try to weaken or destroy a network or cause an interruption in secure data communication by sending loads of unnecessary data packets to the victim nodes and therefore exhibit DoS attack. Different types of DoS attacks may happen in different network layers [28]. At Physical layer, it may cause jamming and tampering, at Data Link layer it causes exhaustion and data collision, at Network layer it causes misdirection and negligence of data and at Transport layer it could perform data flooding and malicious attack [16].

3.2 Sybil Attack:

Another type of WSN attack is Sybil attack. To reduce the fault tolerance, topology maintenance, resource utilization and weaken the routing mechanism the intruder chooses Sybil Attack. In this type of attack a node steals the identities of many nodes to pretend as them to degrade the data integrity and security of the network. The intruder targets the routing mechanism, distributed storage and data aggregation [22] while behaving like a neighbor node and collect all the data for subtasks and data redundancy [23]. But in reality it is only a single malicious node injected intelligently into the specific sensor network to alter valuable information.

3.3 Eavesdropping Attack:

Wireless sensor networks are vulnerable to eavesdropping problem as the data transmission highly depends on assumption that the receiving node faithfully receives and forwards the same transmitted packet containing specified parameters. But during peer-to-peer communication the parameters may be spoofed, replaced, altered, repeated or even diminished by the single frequency or intentional intruders who can easily analyze the traffic flow and fabricate new parameters containing wrong information and transmit them to the sink nodes [18]. Efficient processors with high processing power along with long communication signal range often help intruders in doing so.

3.4 HELLO flood Attack:

In a WSN the network protocols often require HELLO packets broadcasted to the neighbor nodes as signal to identify their consecutive nodes. The laptop-class attackers with long radio frequency and high processing power often target the weak nodes and randomly send HELLO packets to convince them to reply back [13]. As a result, while data transmission to the base stations, the victim nodes try to include the attacker in the

network and broadcast valuable information to it. Such type of attack is known as HELLO flood Attack [24].

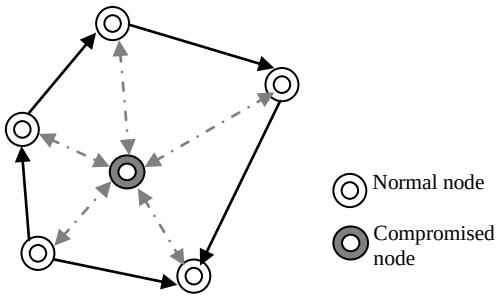

Figure 1: Conceptual diagram of HELLO flood Attack

Figure-1 is a conceptual diagram of HELLO flood attack. Here, the filled-circle represents the Compromised node and the other one represents the Normal sensor node. While the normal nodes are communicating with each other to form a wireless sensor network, the compromised node is randomly sending HELLO packets to each and every node possible (showed by dashed arrows). This keeps the other nodes busy in replying the compromised node and thus the HELLO flood attack is executed.

3.5 Sinkhole Attack:

In this type of attack, the intruder tries to insert itself in between the sensor nodes and the base station as a black-hole [19]. It silently observes the traffic flow of the network and then creates a compromised node as a metaphoric sink node, which will ultimately listen and reply the routing requests and once it get the authentication, it can act as regular sensor nodes. The intruder can spoof, alter and broadcast modified packets to the base station or can even destroy the whole network once it gets the authorization [20].

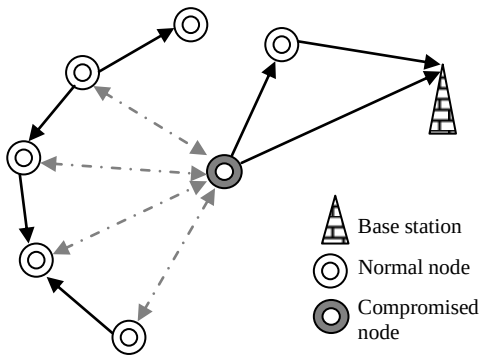

Figure 2: Conceptual diagram of Sinkhole Attack

Figure-2 is a conceptual diagram of Sinkhole attack. Here, the filled-circle represents the Compromised node, the plain-circle represents the Normal sensor node and the triangle represents the Base-station. The compromised node inserted itself in between the base station and the sensor nodes as a black hole and silently affecting the traffic flow of the network. As the diagram shows, the compromised node is listening to the routing requests from the other nodes and replying to the base station like a regular node or making another normal-node of the sensor network believe in it and sending faulty results to that node. Eventually that node sends these faulty reports to the base-station. Thus the whole network obtains false report.

3.6 Wormhole Attack:

In wormhole attack, the intruder records the message received from lower latency links and retransmit them to another location. It does not require conciliation of any of the sensor nodes in a WSN as it cans significantly threaten the network even from the very beginning stage where the nodes are introduced to each other [21]. It can also convince a multi hop sensor network as a single hop by changing the parent nodes. Eventually it misguides the data flow and produce flawed reports.

3.7 Replay Attack:

In this type of attack the intruder interrupts to collect encrypted data packets containing original signature. Once the packets are collected he keeps resending these unaltered data packets continuously, so that the receiving nodes consider them as original data packets. This helps the intruder not only to collect useful secret information but also generate false result by resending old used data.

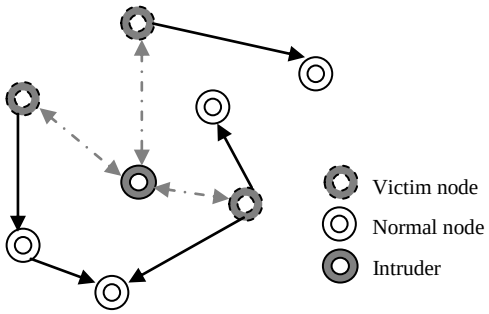

Figure 3: Conceptual diagram of Replay Attack

Figure-3 is a conceptual diagram of Replay attack. Here the filled-circle represents the Compromised node, the plain-circle represents the Normal sensor node and the other one represents the Victim node. The victim node is generally a normal node compromised by the intruder and therefore acting in the favor of it by replaying same old data to other nodes. As a result, data obtained from these victim-nodes are bogus data which helps to generate false reports.

3.8 Selective Forwarding Attack:

Through forwarding attack the intruder tries to reduce the lifetime of the sensor network by exhausting the sensor nodes. As soon as the attacker receives the data packets, he forwards some selective data packets containing all the routing information towards various nodes other than the destination. These data packets need to be resend to the destination which cause high network traffic and increase the power consumption of the sensor nodes. Thus slowly the sensor nodes become exhausted and due to loss of immense energy the network's lifetime decreases

4. SECURITY SOLUTIONS IN WSN

Many researchers have worked with different security issues including attacks and countermeasures and proposed miscellaneous security schemes related to such issues like Zhou and Haas proposed security schemes for ad-hoc networks [10] where as Farr, Smith, Yang and Zhang proposed for mobile ad-hoc networks [11], [12]. But security mechanisms proposed for wireless ad-hoc networks are not appreciable for that of wireless sensor networks due to their architectural differences [14], limitations of the sensor nodes, network density and size. Moreover, numerous various topologies for the sensor nodes,

physical weakness of the wireless sensor networks, especially random intrusion attacks on different layers of the network made it very challenging to build any specific security scheme for wireless sensor network. Therefore, when researchers are busy in ensuring the feasibility of the sensor network, security challenges slipped behind the attention due to high computation problem, repeated data transmission in the network and larger memory location requirement. In this section all the existing proposed security schemes are discussed briefly.

4.1 SPINS:

SPINS, the security protocol for wireless sensor network, is a suit of security building blocks proposed by Adrian Perrig et al. [26] optimized for resource constrained wireless communication and environment. SPIN stands for Sensor Protocols for Information via Negotiation. The two secure building blocks of the suit are: SNEP and µTELSA. While the former one provides data authentication, *confidentiality* and *freshness*, the later one provides *authenticated broadcast* for severely resource-constraint environment.

4.1.1 SNEP:

The Sensor Network Encryption Protocol, in short SNEP uses numerous types of cryptographic primitives like Hash-encryption, Random number generator, symmetric-encryption, Message authentication code etc, assembled in a single block of cipher for reusing the code sevelar times to reduce the overhead on the resource constrained sensor network. The semantic security of SNEP helps to prevent eavesdropping attacks even though the intruder manages multiple encryptions for plain texts. And for such action the randomization technique is used; before using chaining encryption function to encrypt the sending message. The sender precedes the message with a randomly generated bit-string known as Initialization Vector to prevent data-gathering even as a plain text message. Moreover, to avoid added transmission overhead of these extra bits, SNEP provides a shared counter between both the sender and receiver so that it can be shared by both the communicating parties and incremented after transmission of each block [25]. This ensures the security of the channel.

There are a few properties of SNEP like Low communication overhead, Data Authentication, Data freshness, Replay protection, Semantic security etc.

4.1.2 µTELSA

µTELSA stands for Micro version of Timed Efficient Stream Loss-tolerant Authentication. It is a new type of protocol with authenticated broadcasting property for severely resource-constraint environment. Majority protocols for authenticated broadcast are not possibly applicable in wireless sensor networks, because of their mass communication overhead and relying on asymmetric digital signature quality for authentication. µTELSA on the other hand delays the disclosure of the symmetric key while providing efficient authenticated broadcast; which means, it uses symmetric authentication but introduces asymmetry through a delayed disclosure of symmetric key and improve efficiency in broadcasting [27]. µTELSA solves the following in adequacies of TELSA:

> While TELSA authenticates data packets using expensive asymmetric digital signatures, µTELSA uses symmetric authentication mechanism with delayed disclosure of the encryption key.
>
> Since disclosure of the encryption key in every packet requires immense energy/power for both receiving and sending data, µTELSA discloses the key only once per epoch.
>
> µTELSA is cost efficient than TELSA, as it sets a restriction in the number of authenticated message senders.

µTELSA requires a loosely time synchronization between the base station and the sensor nodes for an authenticated broadcast from the base station. The base station computes a message authentication code(MAC) on the data packet with a secret key before sending authenticated data packet to the sensor nodes. When the receiving node receives the packet it verifies the corresponding MAC with the unknown key and ensures that the key is only known by the base station. This assures no intrusion attack took place while data transmission. The packet is then stored by the sensor node in a buffer and waits for the disclosure of the verification key sent from the base station. As soon as the node receives the disclosed key, it verifies whether the key is correct or not. Once the authenticity of the key is confirmed, the node uses it to authenticate the data packet stored in the buffer. Each MAC key belongs to a key chain generated by a one way public function. The nodes in a wireless sensor network perform time synchronization to retrieve authentic keys of the key chain using SNEP building blocks.

4.2 TINYSEC:

TINYSEC is a light weight generic security package with link layer security architecture design by Chris Karlof [28] which provides services comparable to SNEP like message integrity, data authentication and confidentiality, repeated data prevention, data duplication elimination etc. The only difference between TINYSEC and SNEP is TINYSEC does not use any shared counter like SNEP. Rather if it can detect unauthorized packets (even injected in the initial stage), it uses message authentication code to provide basic security, encryption for data confidentiality, prevents data replay and assures semantic security using initialization vector. There are two core security options supported by TINYSEC:

> TINYSEC-AE: This supports authenticated encryption. Here TINYSEC encrypts the data pay-load and authenticates the packet with message authentication code (MAC). The MAC then computes over the packet header along with the encrypted data
>
> TINYSEC-AUTH: This supports only authentication. Here TINYSEC authenticates the entire packet with message authentication code (MAC) and leave the data pay-load unencrypted.

4.3 LEAP:

LEAP stands for Localized Encryption and Authentication Protocol. It is a key-management protocol proposed by S. Zhu, S. Setia, and S. Jajodia [32] and is designed to support network processing and restricting the security impacts of other neighbor nodes related to the specific compromised node at the same time. It is found that different types of data transmitted among the sensor nodes naturally require different types of security mechanisms which a single-key mechanism cannot support. According to Zhu, Setia, and Jajodia, µTELSA fails to provide immediate authentication due to its delayed disclosure of MAC key. Hence it is not completely appropriate for network traffic authentication with single-key mechanism.

A table (Table-1) is provided containing all the proposed security schemes with their major features and the relevant attacks against them.

Table 1: Security schemes for various wireless sensor network attacks

Security scheme	Defense against attack(s)	Major Feature
SPINS	Attacks against Encryption key management and Identity authentication, Denial-of-Service Attack	Data confidentiality, Data integrity, Data authentication, Data freshness, Secure encryption type, Prevention against message replay
SNEP	Message Replay Attack, Spoofing Attack, Data or Information spooling attack, DoS Attack	Lower communication overhead, Data Authentication, Data freshness, Replay protection, Semantic security
µTELSA	Spoofing Attack, Data or Information spooling attack, Selective forwarding attack, DoS Attack	Authenticated broadcasting, Low overhead, Tolerance of message loss, Delayed disclosure of encryption key, Resistance to replay attack, Scalability
TINYSEC	Eavesdropping Attack, Packet Injection, Jamming Attack, Replay Attack	Access control, Data authentication, Message integrity, Replay protection, Confidentiality, Portability and Transparency
LEAP	Forwarding Attack. HELLO-Flood Attack, Sinkhole Attack, Wormhole Attack	Multiple keying mechanisms, Minimize involvement of Base Station, One-way key chain for authentication
RKPS	DoS Attack, Eavesdropping Attack, Sybil Attack, Information transit Attacks	Node to node communication, Limited base-station involvement, High adaptability
PKPS	Message Replay Attack, HELLO flood Attack, Selective forwarding attack	Improved network resilience, Pair-wise key authentication, Multiple key space

LEAP is designed to support four types of key establishment for each sensor node; a group key shared by all the nodes in a sensor network, a cluster key shared by multiple clustering nodes, an individual key shared with the base station and a pair-wise key shared between two sensor nodes. This mechanism minimizes the responsibility of the base station and provides specific protocols to establish and update these keys time to time. LEAP also contains another effective protocol based on one-way key-chain use to authenticate the traffic among the sensor nodes [33].

4.4 RKPS:

RKPS stands for Random Key Pre-distribution Scheme. It is a type of framework containing random set of pre-distributed keys for every single active node in the sensor network, proposed by A. Perrig, H. Chan, and D. Song [34]. RKPS contains three key bootstrapping schemes: the q-composite key scheme, the multi path reinforcement scheme and the random pair wise key scheme. The q-composite scheme assures that pair of nodes shares the same q-keys while establishing secure link and the key pool is short in length. This prevents the eavesdropping attacks as compromising any node needs the hash of shared q-keys. Once the q-keys are assigned, the multi path reinforcement scheme strengthens the security of the key setup by continuous update over multiple independent paths between the selected nodes. This reduces data duplication and resists unexpected node capture. Finally the random pair wise key scheme verifies the node to node identity authentication. Instead of holding n-1 keys the random pair wise key scheme allows only np keys. Each node ID pairs with other random m node IDs and the pair are assigned the secret key. Hence, $n = m / p$ where m = keys on each nodes key ring, n = number of unique node ID and p = probability of two nodes communicating. Thus the random pair wise key scheme reduces the length of the sensor network.

4.5 PKPS:

PKPS stands for Pair-wise Key Pre-distribution Scheme, proposed by Wenliang Du, Yunghsiang S. Han, Jing Deng, Pramod K. Varshney [36] with the target to improve the resilience of the sensor network. The basic concept is, when the number of compromised node is less than the threshold the probability of any other node being affected except the compromised ones is almost zero. The Pair-wise Key Pre-distribution Scheme based on Blom's key pre-distribution method combined with Random Key Pre-distribution method. While Bloom's scheme offered single key space, the pair-wise key pre-distribution scheme offers multiple key space. It is

scalable and flexible enough to allow the sensors use the same memory space. For a sensor network containing 64-bit encryption keys, this method allows up to N = 264 sensor nodes to establish secret keys. Not necessarily all these nodes need to be deployed at the same time. They can join later and still can establish secret keys with the existing nodes. Moreover, the pair-wise key pre-distribution scheme offers multiple hop communication up to 3 hops between node-to-node communication [36].

Other proposed schemes: Jolly, Kuscu, Kokate and Younis proposed a Low-Energy Key Management Protocol [35] for wireless sensor network. It is a cryptographic key management protocol which requires only two symmetric keys to pre-deploy any sensor node. The protocol removes the compromised nodes and lowers the energy consumption overhead. The multi-tire network architecture allows secure sessions between sensor nodes and the gateway only.

Donggang and Peng proposed another framework for establishing pair-wise key distribution among the sensor nodes [37]. They used Polynomial based key pre-distribution technique along with two efficient schemes: A random subset assignment key pre-distribution scheme and a grid based key pre-distribution scheme. These schemes lower the communication overhead, increase the tolerance of node capture and offers high probability to establish Pair-wise keys.

5. CONCLUSION

New technologies expanded in last few years have advanced the architecture on the WSN with more vivacity and exuberance which eventually caused a noticeable increment in the applications of wireless sensor networks. Numerous new protocols and procedures helped to merge both digital and analog sensors to work together for secure data transmission. At the same time, additional new applications of WSN introduced numerous security vulnerabilities of WSN equally increased with the number of applications. In this paper we have studied diverse types of security vulnerabilities and proposed security solutions against them for existing wireless sensor networks (WSN) and showed comparisons among them.

6. REFERENCES

[1] D.E. Culler and W. Hong, “Wireless Sensor Networks”, Communication of ACM, June 2004, Vol. 47, No. 6, pp. 30-33.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,”Wireless Sensor Networks: A survey”, Computer Networks, 2002, pp. 393-422.

[3] J. Undercoffer, S. Avancha, A Joshi and J. Pinkston, “Wireless Sensor Networks”, an edited book,Kluwer Publications, ISBN: 1-4020-7883-8.

[4] P. Adrian, S. John and W. David, “Security in Wireless Sensor Networks”, Communication of ACM, June 2004, Vol 47, Issue No. 6, pp. 53-57.

[5] A.S.K. Pathan, H.K. Islam, S.A. Sayeed, F. Ahmed and C.S. Hong, “A Framework for providing E-Survices to the Rural Area using Wireless Sensor Networks”, IEEE ICNEWS, 2006.

[6] C. Karlof and D. Wagner, “Secure Routing in Sensor Networks: Attacks and Countermeasures” ,Elsevier’s AdHoc Networks Journal, Special Issue on Sensor Network (SNPA), September 2003, pp. 293-315.

[7] H. Chan and A. Perrig, “ Security and privacy in sensor networks ”, IEEE Computer Magazine, October 2003, Vol. 36, Issue. 10, pp. 103–105.

[8] J. Deng, R. Han, and S. Mishra, “Security, privacy, and fault tolerance in wireless sensor networks”, Artech House, August 2005.

[9] E. Shi and A. Perrig, “ Designing Secure Sensor Networks”,Wireless Sensor Networks, IEEE Wireless Communications, December 2004, pp. 38-43.

[10] Zhou, L. and Haas, Z. J., “Securing ad hoc networks”, IEEE Network, December 1999, Vol. 13, Issue. 6, pp. 24 – 30.

[11] Strulo, B., Farr, J., and Smith, A., “Securing Mobile Ad hoc Networks -A Motivational Approach”, BT Technology Journal, July 2003, Vol. 21, Issue. 3, pp. 81 – 89.

[12] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L.,“Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications,February 2004, Vol. 11, Issue. 1, pp. 38 – 47.

[13] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and countermeasures”, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[14] Saleh, M. and Khatib, I. A., “Throughput Analysis of WEP Security in Ad Hoc Sensor Networks”, Proc. The Second International Conference on Innovations in Information Technology, September 2005.

[15] Wood, A. D. and Stankovic, J. A., “Denial of Service in Sensor Networks”, Computer, October 2002, Vol. 35, Issue 10, pp. 54 - 62.

[16] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., “Analyzing interaction between distributed denial of service attacks and mitigation technologies”, Proc. DARPA Information Survivability Conference and Exposition, April 2003, Vol. 1, pp. 26 – 36.

[17] Yuan, L. and Qu, G., “Design space exploration for energy-efficient secure sensor network”, Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, July 2002, pp. 88 – 97.

[18] Charles P. Pfleeger and Shari Lawrence Pfleeger, “Security in Computing”, 3rd edition, Prentice Hall 2003.

[19] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSRMANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[20] Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, “SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks”, Scientific and Technical Research Council of Turkey, from: http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf, 2012

[21] 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, 30th March-3rd April 2003, Vol. 3, pp. 1976 – 1986.

[22] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[23] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[24] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS, Dhaka, 2-4 January, 2006.

[25] Adrian Perrig , Robert Szewczyk , J. D. Tygar , Victor Wen , David E. Culler, "SPINS: security protocols for sensor networks", Wireless Networks, September 2002, Vol.8 No.5, pp.521-534.

[26] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J.D. Tygar, "SPINS: Security protocols for sensor networks", in: International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy 2001.

[27] Xiuli Ren and Haibin Yu, "Security Mechanisms for Wireless Sensor Networks", International Journal of Computer Science and Network security (IJCSNS), March 2006, Vol. 6, No. 3, pp. 155-161.

[28] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," ACM SenSys 2004, Nov. 3-5, 2004, pp. 162-175

[29] Ritu Sharma, Yogesh Chaba, and Yudhbir Singh, "Analysis of Security Protocols in Wireless Sensor Network", International Journal of Advanced Networking and Applications", August 2010, Vol. 2, Issue. 2, pp. 707-713.

[30] M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas, "A Study of Security in Wireless Sensor Networks", MASAUM Journal of Reviews and Surveys", September 2009, Vol. 1, Issue 1, pp. 91-95.

[31] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.

[32] S. Zhu, S. Setia, and S. Jajodia. "Leap: efficient security mechanisms for large scale distributed sensor networks", In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, New York, USA, 2003, pp. 62–72.

[33] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks" International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, Vol. 1, Issue no. 2, pp. 85-95.

[34] A. Perrig, H. Chan, D. Song, "Random Key Pre-distribution Schemes for sensor networks", IEEE 2003 Symposium on Research in Security and Privacy, Berkeley, Canada 2003, pp.197-213.

[35] G. Jolly, M.C. Kuscu, P. Kokate, M. Younis, "A Low-Energy Key Management Protocol for wireless sensor network", 8th IEEE International Symposium on Computers and Communications (ISCC), Turkey 2003, pp.335-340..

[36] Wenliang Du, Yunghsiang S. Han, Jing Deng, Pramod K. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks", 10th ACM Conference on Computer and Communications Security (CCS'03), Washington, DC, USA, October 27–30, 2003, pp. 1-10.

[37] L. Donggang, N. Peng, "Establishing pair-wise Keys in distributed Sensor Networks", 10th ACM Conference on Computer and Communications Security (CCS'03), Washington, DC, USA, October 27–30, 2003, pp. 1-10