A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks

Shio Kumar Singh [1], M P Singh [2], and D K Singh [3]

[1]*Maintenance Engineering Department (Electrical), Tata Steel Limited, Jamshedpur – 831001, Jharkhand, India,*

[2] *Computer Science and Engineering Department, National Institute of Technology, Patna, Bihar, India,*

[3] *Electronics and Com. Engg. Dept, Birsa Institute of Technology, Sindri, Dhanbad –828123, Jharkhand, India,*

Abstract: The severe constraints and demanding deployment environments of wireless sensor networks make security for these systems more challenging than for conventional networks. However, several properties of sensor networks may help address the challenge of building secure networks. The unique aspects of sensor networks may allow novel defenses not available in conventional networks.

In this paper, we investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks.

Keywords: Wireless Sensor Networks (WSNs), Security, Threats, Attacks,

I. INTRODUCTION

Wireless sensor network (WSN) is a heterogeneous system combining thousands to millions of tiny, inexpensive sensor nodes with several distinguishing characteristics. It has very low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions [2], [3], [4], [5], [6], [7]. However, WSNs form a particular class of ad hoc networks that operate with little or no infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network [1]. However, designing security protocols is a challenging task for a WSN because of the following unique characteristics:

- Wireless channels are open to everyone and has a radio interface configured at the same frequency band. Thus, anyone can monitor or participate in the communication in a wireless channel. This provides a convenient way for attackers to break into a network.
- As in the case of the Internet, most protocols for WSNs do not consider necessary security mechanisms at their design stage. On the other hand, most protocols are publicly known due to the needs for standardization. For these reasons, attackers can easily launch attacks by exploiting security holes in those protocols.
- The constrained resources in sensor nodes make it very difficult to implement strong security algorithms on a sensor platform due to their complexity. In addition, large numbers of sensor nodes pose the demand for simple, flexible, and scalable security protocols.
- A stronger security protocol costs more resources in sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off has to be made between security and performance. However, weak security protocols may be easily broken by attackers.
- A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, it may face various potential attacks.

In this paper, we discuss the most common security services for WSNs. The paper is structured as follows. Section 2 focuses on the critical security issues in WSN. Section 3 explores various threats and attacks compromising the availability of network services. Section 4 reviews the related works and proposed schemes concerning security in WSN. Finally, we conclude the chapter in Section 5.

II. SECURITY ISSUES IN WSN

A sensor network is a special type of Ad hoc network. So it shares some common property as computer network. There are usually several security requirements to protect a network [1]. These requirements should be considered during design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. The security requirements [1], [8], [9], [10], [11], [12] of a wireless sensor network can be classified as follows:

A. Data Confidentiality

Data confidentiality in networking is most challenging task in network security. The major problem is that radio spectrum is an open resource and can be used by anyone equipped with proper radio transceivers. An attacker can eavesdrop on the packets transmitted in the air as long as he is able to keep track of the radio channels used in the communication. An attacker can capture a node, dig into it

with special tools, and find useful data. The attacker can also derive the secrets in a node without capturing it, which can be done by analyzing the secret data collected from other compromised nodes and/or packet protocol data units (PDUs). Under the attacker's control, the new compromised node can be used to launch more malicious attacks.

Confidentiality is an assurance of authorized access to information. It is the ability of the network to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential [13]. Thus, it ensures the protection of sensitive information and not revealed to unauthorized third parties. Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. In such applications, nodes communicate highly sensitive data. The standard approach for keeping confidentiality is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. As per TinySec [17], cipher block chaining (CBC) is the most appropriate encryption scheme for sensor networks.

B. Data Authenticity

In addition to modifying existing packets, an attacker can directly inject packets if he knows the packet format defined in the network protocol stack. The injected packets can carry false information, which may be accepted by receiving nodes. Applications deployed in a WSN, for example, environmental monitoring or object tracking, can be disrupted by the false information. Routing protocols can fail due to the false routing information. The Sybil attack [15] is a typical example of packet injection.

Data authenticity is an assurance of the identities of communicating nodes. WSN communicates sensitive data to help in many important decisions making. Thus, it is very important for every node to know that a received packet comes from a real sender. Otherwise, the receiving node can be cheated into performing some wrong actions. Also, authentication is necessary during exchange of control information in the network. The standard approach for keeping authenticity is through the use of message authentication code, challenge response, signature, authenticating public key, broadcast and multicast authentication, etc.

C. Data Integrity

Transmission errors are inherent in wireless communications because of the instability of wireless channels, which is due to many reasons, for example, channel fading, time-frequency coherence, and inter-band interference. Errors can also happen in each forwarding node because no electronic devices are perfect. When the operation conditions, for example, temperature or humility, are out of the normal range, electronic devices can run into malfunction, which can cause errors in packets. Those errors may not be noticed by the forwarding node and thus those error packets may still be sent out, causing troubles at down-stream nodes. In hostile environment, data in transit can also be changed by an attacker who can modify a packet before it reaches the receiver. This can cause many problems. The attacker can simply introduce radio interference to some bits in transmitted packets to change their polarities. The unintelligible packets will be dropped at the receiver, leading to a simple Denial of Service (DoS) attack [14]. More serious damages can be caused if the attacker understands the packet format and the semantic meaning of the communication protocol. In that case, the attacker can modify a packet to change its content so that the receiver obtains wrong information. In a WSN, for example, a packet containing the location of an important event can be modified so that a wrong location is reported to the base station. Control and management packets can be changed so that nodes have inconsistent knowledge on the network topology, which causes many routing problems. A packet bearing errors is useless and causes extra processing at the sender and the receiver.

Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident. Thus, integrity is an assurance that packets are not modified in transmission. This is a basic requirement for communications because the receiver needs to know exactly what the sender wants her to know. However, this is not an easy task in wireless communications. The standard approach for ensuring data integrity is through the use of message integrity code, etc.

D. Data Freshness

All information describes a temporary status of an object and thus is valid in only a limited time interval. Therefore, when a node receives a packet, it needs to be assured that the packet is fresh. Otherwise, the packet is useless because the information conveyed in it is invalid. Packet replaying is a major threat to the freshness requirement in network communications. An attacker can intercept a packet from a network, hold it for any amount of time, and then reply it into the network. The out-dated information contained in the packet can cause many problems to the applications deployed in the network. In a WSN, for example, a packet indicating the emergence of an event will conflict with an old packet containing no indication of the event. If some old routing control packets are replayed, sensor nodes will be put into a chaos about the network topology and thus the routing protocol will fail. In addition to the replay in time dimension, packets can also be replayed in space dimension. An example is the Wormhole attack in WSNs [16].

Thus, even if confidentiality and data integrity are assured we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. In order to ensure the freshness of packet, a timestamp can be attached to the packet. A receiving node can compare the timestamp in the packet with its own time clock and determine whether the packet is valid or not

E. Availability

Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network. Any problem in a network can result in the degradation of the network functionality and thus compromise the network availability, leading to the DoS [14].

Availability is an assurance of the ability to provide expected services as they are designed in advance. It is a very comprehensive concept in the sense that it is related to almost every aspect of a network. The standard approach for keeping confidentiality is through the use of selective forwarding, multipath routing, etc.

III. SECURITY THREATS AND ATTACKS IN WSN

A. Security Threats

A threat is a circumstance or event with the potential to adversely impact a system through a security breach and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk. There can be many potential threats to WSNs, for example, power drainage, physical tampering, extinction immediately upon deployment due to the hostile environment or deliberate attempts to subvert a node by breaching the security. The categories of the threats could be (a) Passive Information Gathering, (b) Subversion of node or Insertion of a false node, (c) node malfunction, (d) node outage, (e) message corruption, (f) denial of service, or (g) traffic analysis [22].

According to Karlof et. al. [19], threats in wireless sensor network can be classified into the following categories:

- **External versus internal attacks:** The external (outsider) attacks are from nodes which do not belong to a WSN. An external attacker has no access to most cryptographic materials in sensor network. The internal (insider) attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. The inside attacker may have partial key material and the trust of other sensor nodes. Inside attacks are much harder to detect. External attacks 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 and who then use one or more laptop-class devices to attack the network.
- **Passive versus active attacks:** Passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a WSN. The active attacks involve some modifications of the data steam or the creation of a false stream in a WSN.
- **Mote-class versus laptop-class attacks:** In mote-class (sensor-class) attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like laptop, etc. and can do much more harm to a network than a malicious sensor node. These types of attackers can jam the radio link in its immediate vicinity. An attacker with laptop-class devices have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and hence they can affect much more than an attacker with only ordinary sensor nodes. A single laptop-class attacker might be able to eavesdrop on an entire network.

B. Attacks

Wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. These attacks are normally due to one or more vulnerabilities at the various layers in the network [22]. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected [21]. The security of the WSNs is compromised due to the attacks. 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 [12]. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. As illustrated in Figure 1, attacks on the computer system or network can be broadly classified [18] as interruption, interception, modification and fabrication.

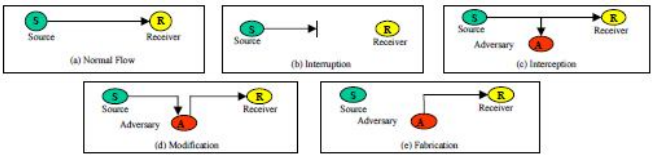


Fig. 1 Attack security classes

Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. ***Interception*** is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it. Modification is an attack on integrity. ***Modification*** means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with bogus data. ***Fabrication*** is an attack on authentication. In

fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed. Some of the critical attacks [12], [26], are categorized as follows:

Denial of Service (DoS): Denial of Service (DoS) [23], [27], [28] is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks. Sensor networks being very energy-sensitive and resource-limitation, they are very vulnerable to DoS attacks. Wood and Stankovic [14] explored various DoS attacks that may happen in every network layers of sensor networks. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization.

Sybil: Sybil attack is defined as a malicious device illegitimately taking on multiple identities. In Sybil attack [24], an adversary can appear to be in multiple places at the same time. In other words, a single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of legitimate nodes. Figure 2 demonstrates Sybil attack where an adversary node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as to 'D' so when 'A' wants to communicate with 'F' it sends the message to 'AD'. Sybil attack is a harmful threat to sensor networks. It poses a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. The Sybil attack can disrupt normal functioning of the sensor network, such as multipath routing, used to explore the multiple disjoint paths between source-destination pairs. It can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersity and multipath.

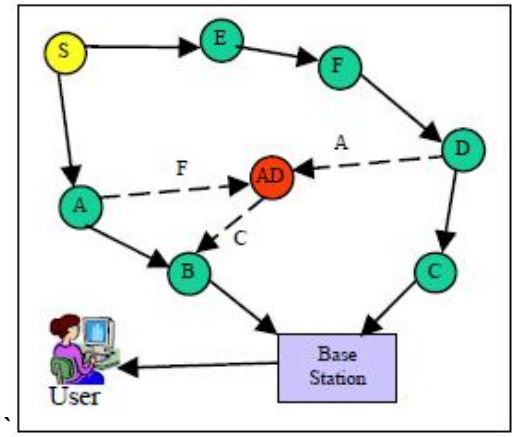


Fig. 2 Sybil attack

Sybil attack problem was first presented in the peer-to-peer distributed systems by Douceur [24] wherein it was pointed out that it could defeat the redundancy mechanisms of the distributed storage systems. Newsome et al. [15] analyzed the threat posed by the Sybil attack to wireless sensor networks. They established a classification of different types of the Sybil attack, proposed several techniques to defend against the Sybil attack, and analyzed their effectiveness quantitatively.

Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. It can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [15]. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack.

Sinkhole (Blackhole): In sinkhole attacks, a malicious node acts as a blackhole [29] to attract all the traffic in the sensor network through a compromised node creating a metaphorical sinkhole with the adversary at the center. A compromised node is placed at the centre, which looks attractive to surrounding nodes and lures nearly all the traffic destined for a base station from the sensor nodes. Thus, creating a metaphorical sinkhole with the adversary at the center, from where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. Figure 3 demonstrates sinkhole attack where 'SH' is a sinkhole. This sinkhole attracts traffic from nearly all the nodes to rout through it.

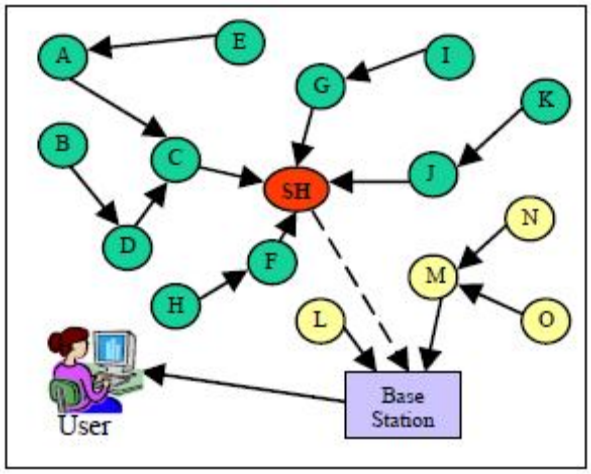


Fig. 3 An example of Sinkhole (Blackhole) attack

The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

Hello flood: Hello flood attack [19] uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. This assumption may be false. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbor, so that all the nodes will respond to the HELLO message and waste their energy. Figure 4 illustrates how an adversary node 'AD' broadcast hello packets to convince nodes in the network as neighbor of 'AD'. Though some node like I,H,F are far away from 'AD' they think 'AD' as their neighbor and try to forward packets through it which results in wastage of energy and data loss.

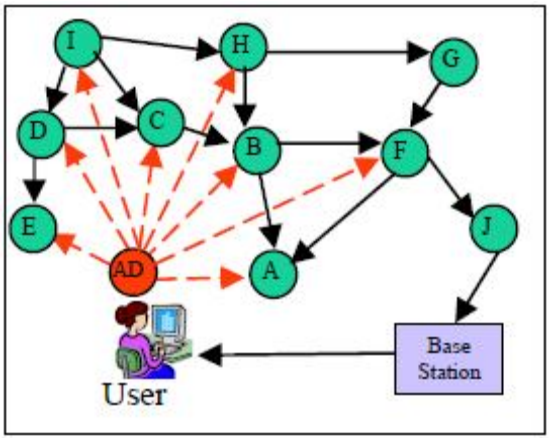


Fig. 4 Hello flood attack

In a HELLO flood attack, every node thinks that the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes.

Wormhole: Wormhole attack [16], [25] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. In the wormhole attack, an adversary (malicious nodes) eavesdrop the packet and can tunnel messages received in one part of the network over a low latency link and retransmit them in a different part. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms wormholes in a sensor network. The tunneling or retransmitting of bits could be done selectively. Figure 5 demonstrates Wormhole attack where 'WH' is the adversary node which creates a tunnel between nodes 'E' and 'I'. These two nodes are present at most distance from each other.

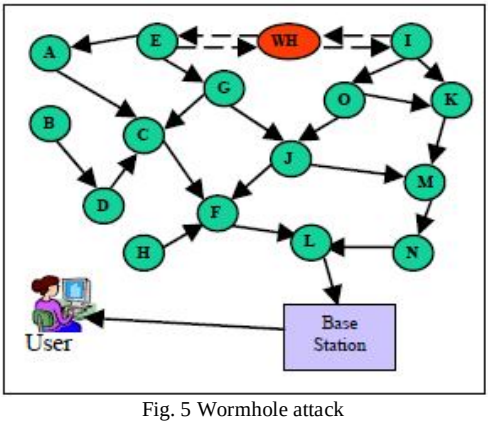


Fig. 5 Wormhole attack

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 neighbors, leading

to quick exhaustion of their energy resources. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor's network protocols.

Wormhole attack is a significant threat to wireless sensor networks, because this type of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

IV. RELATED WORKS AND SECURITY SOLUTIONS IN WSN

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world [7]. In view of resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it becomes very challenging task to apply security schemes in wireless sensor networks. While much research has focused on making these networks feasible and useful, security has received little attention. Researchers have been trying to resolve security issues [20]. Most of the existing security mechanisms require intensive computation and memory. Many security mechanisms require repeated transmission/communication between the sensor nodes which are further drawn in their resources. In this section, we review some of the popular security solutions and combat some of the threats to the sensor networks.

A. SPINS

Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig *et al.*[36] in which security building blocks optimized for resource constrained environments and wireless communication. SPINs has two secure building blocks: (a) sensor network encryption protocol (SNEP) and (b) µTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments.

SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. Since sending data over the RF channel requires more energy, all cryptographic primitives such as encryption, MAC, hash, random number generator, are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used reduces the overhead on the resource constrained sensor network. SNEP provides number of advantages such as low communication overhead, semantic security which prevents eavesdroppers from inferring the message content from the encrypted message, data authentication, replay protection, and message freshness.

µTesla is a new protocol which provides authenticated broadcast for severely resource-constrained environments. In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTesla protocols provide efficient authenticated broadcast [39], [40] and achieves asymmetric cryptography by delaying the disclosure of the symmetric keys. µTesla constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. µTESLA solves the
following inadequacies of TESLA in sensor networks:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA discloses the key once per epoch.
- It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders.

B. TINYSEC

TinySec is link layer security architecture for wireless network, which was designed by Karlof *et al.* [17]. It provides similar services as of SNEP, including authentication, message integrity, confidentiality and replay protection. It is a lightweight, generic security package that can be integrated into sensor network applications. A major difference between TinySec and SNEP is that there are no counters used in TinySec.
TinySec provides the basic security properties of message authentication and integrity using MAC, message
confidentiality through encryption, semantic security through an Initialization Vector and replay protection.

TinySec supports two different security options: authenticated encryption (TinySec- AE) and authentication only (TinySec-Auth). For authenticated encryption (TinySec-AE), TinySec uses cipher block chaining (CBC) mode and encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode (TinySec-Auth), TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.

C. LEAP

Localized encryption and authentication protocol (LEAP) Protocol [41] is a key management protocol for sensor networks. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication. In addition, LEAP is to meet several security and performance requirements that are considerably more challenging to sensor networks. Design of the LEAP protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements. LEAP has the following properties:

- LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy efficient, and minimizes the involvement of the base station.
- LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains.
- Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node.

In Table 1, we have summarized various security schemes along with their main properties for wireless sensor network.

TABLE 1
SUMMARY OF VARIOUS SECURITY SCHEMES FOR WIRELESS SENSOR NETWORKS

Security Schemes	Attacks Deterred	Network Architecture	Major Features
JAM	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes.
Wormhole based	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Use wormholes to avoid jamming
Radio Resource Testing. Random Key Pre-distribution	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and code attestation for detecting Sybil entity
Bidirectional Verification, Multi-path, multi-base station routing	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On communication Security	Information or Data Spooling	Traditional wireless sensor network	Efficient resource management, Provide the network even if part of the network is compromised
TIK	Wormhole Attack Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Kay Pre-distribution	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing. Takes advantage of the broadcast inter-radio behavior to watch neighbor transmission and detect blackhole attacks
Tiny Sec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focus on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

V. CONCLUSION

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, we have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network security for WSNs is still a very fruitful research direction to be further explored.

REFERENCES

1. Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.
2. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", *International Journal of Advanced Networking and Application (IJANA)*, Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.
3. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", *International Journal of Wireless & Mobile Networks (IJWMN)*, Aug. 2010, vol. 2, no. 3, pp. 49-61.
4. 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.
5. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey" *International Journal of Computer Science and Engineering Survey (IJCSES)*, November 2011, Vol. 1, issue no. 2, pp. 63-83.
6. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", *Global Journal of Computer Application and Technology (GJCAT)*, Jan. 2011, vol. 1, no. 1, pp. 57-65.
7. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", *International Journal of Grid and Distributed Computing (IJGDC)*, December 2010, vol. 3, no. 4, pp. 89-104.
8. E. Yoneki and J. Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role", Technical Report, 2005. *http://www.cl.cam.ac.uk/TechReports*, ISSN 1476-2986.
9. J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security - a survey", *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, CRC Press, 2007.
10. L.L. Fernandes,"Introduction to Wireless Sensor Networks Report", *University of Trento*. 2007, http://dit.unitn.it/~fernand/downloads/iwsn.pdf
11. A. T. Zia, "A Security Framework for Wireless Sensor Networks". 2008, http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf
12. 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.
13. M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas, "A Study of Security in Wireless Sensor Networks", *MASAUM Journal of Reviews and Surveys"*, Sept. 2009, vol. 1, Issue 1, pp. 91-95.
14. A.D. Wood and J. Stankovic, "Denial of service in sensor network", *IEEE Computer Magazine*, vol. 5, no. 10, Oct. 2002, pp. 54-62.
15. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses" in *Proceedings of the 3rd IEEE International Symposium on Information Processing in Sensor Networks (IPSN'04)*, Berkley, CA, Apr. 2004, pp. 259-268.
16. Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03)*, vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.
17. Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: A Link Layer security Architecture for Wireless Sensor Networks", *ACM SenSys 2004*, Nov. 3-5, 2004, pp. 162-175.
18. W. Stallings, "Cryptography and Network Security Principles and Practice", *Cryptography Book, 2nd Edition, Prentice-Hall*, 2000, 0-13-869017-0.
19. C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network (SNPA)*, Sept. 2003, pp. 293-315.
20. Ritu Sharma, Yogesh Chaba, and Yudhbir Singh, "Analysis of Security Protocols in Wireless Sensor Network", International Journal of Advanced Networking and Applications", Aug. 2010, vol. 2, Issue 2, pp. 707-713.
21. 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.
22. Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, and John Pinkston, "Wireless Sensor Networks", an edited book, Kluwer Publications, ISBN: 1-4020-7883-8
23. M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", *SETIT 2007*.
24. J.R. Douceur, "The Sybil Attack", *in 1st International Workshop on Peer-to-Peer Systems (IPTPS'02)*, March 2002, LNCS 2429, 2002, pp. 251-260.
25. Y.C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," *Department of Computer Science, Rice University, Tech. Rep. TR01-384*, June 2002.
26. H.K. Kalita and A. Kar, "Wireless Sensor Networks Security Analysis", *International Journal of Next-Generation Networks (IJNGN)*, vol. 1, no. 1, Dec. 2009, pp. 01-09.
27. W.J. Blackert, D.M. Gregg, A.K. Castner, E.M. Kyle, R.L. hom, and R.M. Jokerst "Analyzing interaction between distributed denial of service attacks and mitigation technologies", *Proc. DARPA Information Survivability Conference and Exposition*, Vol. 1, 22-24 April, 2003, pp. 26 – 36.
28. B.T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks", *Canadian Conference on Electrical and Computer Engineering*, Vol. 2, 2-5 May 2004, pp. 901 – 904.
29. B.J. Culpepper and H.C. Tseng, "Sinkhole intrusion indicators in DSR MANETs", *Proc. First International Conference on Broad band Networks*, 2004, pp. 681 – 688.
30. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks", *IEEE Journal on Selected Areas in Communications*, Volume 23, Issue 4, April 2005, pp. 839 – 850.
31. L. Yuan and G. Qu, G, "Design space exploration for energy-efficient secure sensor network", *Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors*, 2002, 17-19 July 2002, pp. 88 – 97.
32. G. Jolly, M.C. Kuscu, P. Kokate, and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks", *Proc. Eighth IEEE International Symposium on Computers and Communication*, 2003. (ISCC 2003). vol.1, pp. 335 - 340.
33. M. Younis, M. Youssef, and K. Arisha, "Energy-aware routing in cluster-based sensor networks" Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.
34. A.D. Wood, J.A. Stankovic, and S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", *24th IEEE Real-Time Systems Symposium, (RTSS)*, 2003, pp. 286-297.
35. M. Cagalj, S. Capkun, and J.P. Hubaux, "Wormhole-based Anti-Jamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf.
36. A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS:

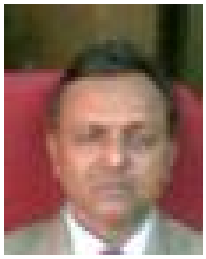
Security Protocols for Sensor Networks", *Wireless Networks*, vol. 8, no. 5, 2002, pp. 521-534.
37. S.S. Kulkarni, M.G. Gouda, and A. Arora, "Secret instantiation in adhoc networks," *Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks*, May 2005, pp. 1–15.
38. M.A. Hamid, M.O. Rashid, and C.S. Hong, "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in *IEEE ICNEWS 2006*, 2-4 January, Dhaka.
39. Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar, "Efficient and secure source authentication for multicast", *In Network and Distributed System Security Symposium, NDSS 01*, February 2001.
40. Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song, "Efficient authentication and signing of multicast streams over lossy channels" *In IEEE Symposium on Security and Privacy*, May 2000.
41. S. Zhu, S. Setia, and S. Jajodia. "Leap: efficient security mechanisms for largescale distributed sensor networks", *In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, New York, USA, 2003, pp. 62–72.

SHORT BIOGRAPHY

Shio Kumar Singh is Head of Maintenance Engineering Department (Electrical) at Tata Steel Limited, Jamshedpur, India. He received degrees in both Electrical and Electronics engineering, as well as M.Sc.(Engg.) in Power Electronics from Regional Institute of Technology, Jamshedpur, India. He also obtained "Executive Post Graduate Diploma in International Business" from Indian Institute of Foreign Trade (IIFT), New Delhi, India. He is an accomplished academician with rich industrial experience in design, development, implementation and marketing & sales of IT, Automation, and Telecommunication solutions, Electrical & Electronics maintenance, process improvement initiatives (Six-sigma, TPM, TOC), and Training & Development in a distinguished career spanning over 30 years. He has published number of papers in both national and international journals and has presented these in various seminars and symposiums.

He is author of several engineering books such as Database Management System, Industrial Instrumentation and Control, and Process Control Systems published by Pearson Education, McGraw-Hill, and Prentice-Hall of India. He is widely traveled and has visited various industries in Europe and South Asian countries for study and marketing of process automation systems. He has been conferred the Eminent Engineer and Distinguished Engineer Awards by The Institution of Engineers (India) for his contributions to the field of computer science and engineering. He is a Chartered Engineers and also a Fellow Member (FIE) of The Institution of Engineers (India).

Dr. M. P. Singh is an Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology Patna, Bihar, India. He has experience of five years. He has authored number of papers which have been published in both national and international journals. His research interest is in the area of Wireless Sensor Network, Mobile Computing



Dr. Dharmendra K Singh is presently working as Head, Department of Electronics and Communication & Information Technology, BIT Sindri, Dhanbad. He has more than 20 years of teaching experience. He is heading the department of Electronics and Communication & Information technology since 2002. He is instrumental in starting the curriculum on information technology. He has published more than 35 papers in journals and conferences. He has already supervised 01 thesis in computer Science & Engg and 05 research scholars are presently enrolled for their doctoral degree. The area of research he works are Coding theory, cryptography, optical Amplifiers, Photonic Crystal Fibers, e-Governance and Educational Planning. He is member and conveners of various computerization programs of BIT Sindri, Vinoba Bhave University, Ranchi University. He is also a Fellow Member (FIE) of The Institution of Engineers (India).