Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security in Wireless Sensor Networks

By Koffka Khan, Wayne Goodridge & Diana Ragbir

The University of the West Indies

Abstract - Wireless Sensor Networks (WSNs) pose a new challenge to network designers in the area of developing better and secure routing protocols. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. However, sensor networks are not traditional computing devices, and as a result, existing security models and methods are ill suited. The security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. With the recent surge in the use of sensor networks, for example, in ubiquitous computing and body sensor networks (BSNs) the need for security mechanisms has a more important role. Recently proposed solutions address but a small subset of current sensor network attacks. Also because of the special battery requirements for such networks, normal cryptographic network solutions are irrelevant. New mechanisms need to be developed to address this type of network.

Keywords : *wireless sensor networks, routing, protocol, security, cryptographic.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Security in Wireless Sensor Networks

Koffka Khan [α], Wayne Goodridge [σ] & Diana Ragbir [ρ]

Abstract - Wireless Sensor Networks (WSNs) pose a new challenge to network designers in the area of developing better and secure routing protocols. Many sensor networks have mission-critical tasks, so it is clear that security needs to be taken into account at design time. However, sensor networks are not traditional computing devices, and as a result, existing security models and methods are ill suited. The security issues posed by sensor networks represent a rich field of research problems. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. With the recent surge in the use of sensor networks, for example, in ubiquitous computing and body sensor networks (BSNs) the need for security mechanisms has a more important role. Recently proposed solutions address but a small subset of current sensor network attacks. Also because of the special battery requirements for such networks, normal cryptographic network solutions are irrelevant. New mechanisms need to be developed to address this type of network.

Keywords : wireless sensor networks, routing, protocol, security, cryptographic.

I. Introduction

Wireless Sensor Networks (WSNs) are made up of a group of sensor nodes; each node is equipped with its own sensors and actuators, radio frequency transceiver, power source, processing capability – Digital Signal Processing (DSP) chips [1] or CPUs and memory [2], which can monitor and sense changes in the environment and forward that data to a sink or base station in the network. Sensor nodes can measure a variety of properties in the environment based on the sensors and actuators that are built into them. These include physical properties – pressure, temperature, humidity, flow; motion properties – acceleration, velocity, position; contact properties – force, strain, vibration, slip, torque; presence – proximity, motion, tactile/contact, distance/range; biochemical; identification – vision, retinal scans, fingerprints; noise levels; and lighting conditions [1].

The sensors in-built into the nodes depend on the specific application area in which the WSN is implemented. WSNs have been used traditionally in military applications but other areas include environmental such as ocean, wildlife, wildfire, and pollution monitoring; medical such as wearable sensors – temperature measurement, respiration and heart monitors, glucose sensors, and implanted sensors – endoscope capsule, brain liquid pressure sensor, cardiac arrhythmia monitor; crisis management; smart spaces; building safety and earthquake monitoring; water quality monitoring; and machinery performance monitoring in production and delivery [5], [10].

Given the broad range of applications, there is intensive, active research being undertaken in WSNs involving networking, hardware and system design, distributed algorithms, data management, and security. At present most of the major wireless sensor network (WSN) routing protocols are insecure, because during their initial development very little emphasis was put around security as a foremost goal. However it became a relevant issue with the deployment of such networks, for example, in border control systems. Due to the complexity involved addressing the security issues of WSNs is non-trivial to fix. Emphasis must be placed around the routing protocols of sensor networks themselves and security must be designed using a bottom-up approach, that is, it must be designed into the protocol from scratch or during the earliest possible development time for such networks.

There are specific classes of attacks which affect wireless sensor networks and are applicable to only such types of networks. This is because wireless sensor networks have special characteristics (security protocols cannot maintain much state, communication bandwidth is extremely dear, power is the scarcest resource of all, which distinguish themselves from other types of networks, for example, mobile ad hoc networks. Further to this countermeasures and design considerations for sensor networks (we must discard many preconceptions about network security) need to be proposed or developed to address the special needs for such networks. Because power is the most important consideration when deploying such networks, public key cryptography cannot be used as it is too expensive. Even fast symmetric-key ciphers must be used sparingly. Hence some ad-hoc network security mechanisms based on key cryptography are unsuitable for sensor networks.

New security mechanism must be proposed for wireless sensor networks. In I we introduce the problem statement. Attacks on sensor network routing are discussed in I. Section III shows some countermeasures and conclusions are given in IV.

II. Problem Statement

The characteristics of WSNs that make security a difficult challenge, in terms of being different from security in traditional networks, are their limited power,

Author α : Koffka Khan. E-mail : koffka.khan@sta.uwi.edu
Author σ : Wayne Goodridge. E-mail : wayne.goodridge@sta.uwi.edu

communication and processing or computation capabilities [5], [11]. Additional challenges to security in WSNs are that they operate in real-time as opposed to not real-time, have dynamically changing sets of resources as opposed to a fixed set of resources, the aggregate behavior of all nodes is important as opposed to a wired network where every node is important, their location is critical as opposed to location independent networks and finally, they utilize sensors and actuators instead of screen and mice as interfaces to the nodes. WSNs also communicate wirelessly, are deployed in an ad hoc fashion and are self-organized.

Römer and Mattern in [3] offered dimensions in the design of WSNs which could be used to better understand what security measures should be implemented in a given WSN. The first dimension of design is network size – nodes can range from a few to thousands and the size of the network affects the design of protocols and algorithms. The lifetime of WSNs can be measured in hours or up to years and impacts the power efficiency and robustness of nodes. Connectivity within a WSN can be fully connected all the time, have intermittent connectivity or designed to be sporadic – nodes occasionally enter the transmission range of other nodes. Connectivity has an influence on methods of data gathering and choice of communication protocols.

Furthermore, coverage within a WSN can be sparse, dense, or redundant based on the degree of coverage of the nodes in the network. High coverage (redundant nodes) is important to the robustness of the network. The topology of the WSN is another dimension and can be single-hop, star, tree or graph; this affects the diameter of the network which influences latency, robustness and capacity. Heterogeneity of the WSN means either it consists of homogenous nodes in terms of hardware and software or heterogeneous, where nodes can be different devices with various functions. This affects complexity and security of the system. Complexity and security of the system is also affected by the cost, size, resource and energy dimensions of a WSN.

Other dimensions include mobility – degree of mobility, frequency of movement, active or passive movement; deployment – one-time or continuous set up of nodes, random locations or chosen spots; communication modality – radio, light, inductive, capacitive or sound transmissions; and finally quality of service (QoS) – robustness, real-time constraints, eavesdropping resistance, tamper resistance and unobtrusiveness or stealth. These dimensions also impact security measures in various ways.

These unique characteristics and design dimensions of WSNs pose constraints to applying existing security approaches and provide obstacles in developing security defenses [4]. These unique characteristics and dimensions contain several vulnerabilities of WSNs to which threats can occur. When threats are carried out, they are considered attacks.

Generally radio links are insecure. Nodes can be either a general type or one with more capabilities (generally the base stations with more transmitting power). The adversary can deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes or can "turn" a few legitimate nodes into threat agents. Since sensor nodes were not developed with security in mind these nodes are not tamper resistant. Base stations are generally assumed to have a higher trust factor, while aggregation points can be suspect of being threat agents.

Threat models are categorized as being either mote-class attacks versus laptop-class attacks or outsider attacks versus insider attacks. For WSNs the security goals that should be prioritized are integrity, authenticity and availability of messages.

III. Sensor Network Routing Attacks

First, several threat models will be explained, followed by the attacks categorized by the network architecture layer to which they apply. There are two types of attackers, mote class and laptop class. Mote class attackers only have access to a few nodes, whereas, laptop class attackers have access to more powerful devices such as laptops with great battery power, powerful CPUs, sensitive antennas and high power radio transmitters. Two types of attacks include insider and outsider attacks. In an insider attack, the attacker is considered to be an authorized member of the network, whereas, outsider attackers do not have authorized access to the network. Additionally, insider attacks can take place from laptops using stolen data from legitimate nodes or from compromised sensor nodes.

Attacks in the first four layers of the network architecture are now discussed [7], [12]. The attacks in the Physical layer are Jamming and Tampering [7]. Jamming occurs when an adversary blocks the radio frequencies that legitimate nodes are using. A complete Denial of Service (DoS) (cf. Figure 1) occurs if the adversary blocks the entire network. Tampering refers to physical damage, replacement or modification of a node or part of a node. Damage to sensors, modification of circuitry, replacement of a node's hardware or of the entire node, and replacement of sensors with malicious sensors are examples of tampering. Additionally, an adversary can interrogate nodes electronically to gain access to cryptographic data and information on accessing other communication layers.

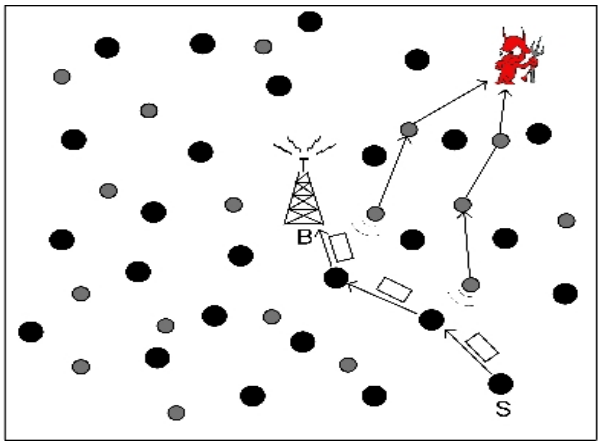

Fig.1 : Denial of Service Attack

Collisions, Unfairness and Exhaustion are attacks in the data link layer [7]. Collision is a type of link layer jamming. Part of the transmission is corrupted so that a mismatch in the checksum occurs. This leads to a disruption of the packet. Also, an attacker could deny access to a channel, intentionally, leading to more collisions in other channels or to packets never being received at the destination.

Unfairness happens when MAC priority schemes are abused, which leads to degradation of service though loss of real-time deadlines. Exhaustion attacks aim to drain power resources of the node.

In the data link layer, repeated retransmissions even after late collisions can drain power. Also, compromised nodes can self-sacrifice by continuously asking for access to a channel; its neighbors are then forced to respond with a 'clear to send' message, draining resources of many nodes.

The network layer has the most kinds of attacks - spoofed, altered or replayed information; Sybil attacks; sinkhole attacks; selective forwarding; hello flood attacks; wormholes; and acknowledgement spoofing [7]. Firstly, Spoofed, Altered or Replayed Information is the most direct attack. Here, the attacker complicates the network and many negative consequences may result including the creation of routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, replay attacks (cf. Figure 2), increase end-to-end latency, etc.

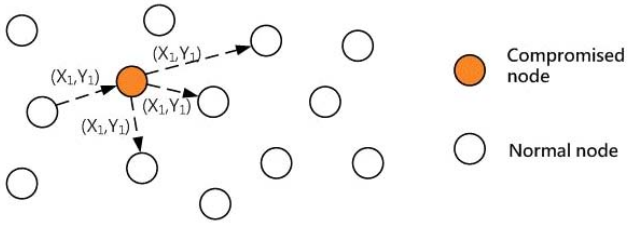

Fig. 2 : Replay Attack

The Sybil attack works by using a compromised node to pose multiple identities to the network in order to confuse geographic routing protocols, since the adversary appears to be in multiple locations at once (cf. Figure 3). The Sybil attack targets fault tolerant schemes such as multipath routing, dispersity, distributed storage and topology maintenance.

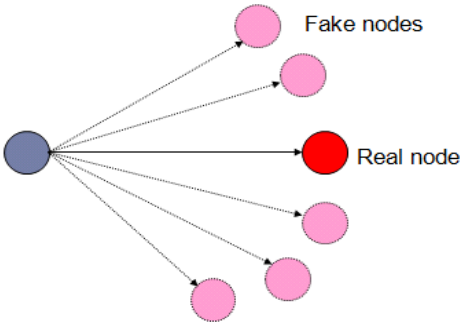

Fig. 3 : Sybil Attack

In Sinkhole attacks, the goal is to bait traffic to a malicious part of the network (cf. Figure 4). This is done by first making a compromised node look appealing to its neighbors in terms of routing of packets. The compromised node advertises low latency routes and fooled legitimate neighbor nodes forward their packets to the lying node, thus creating a sinkhole in the network.

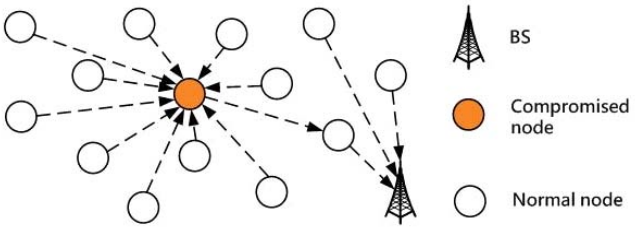

Fig. 4 : Sybil Attack

In Selective Forwarding, an adversary includes itself in the data flow path of interest. (cf. Figure 5) The adversary can then choose not to forward packets sent to it, thus creating a kind of black hole. Instead, the adversary can drop packets that come from a specific source while continuing to route all other packets reliably. In this case, the attack is harder to detect.

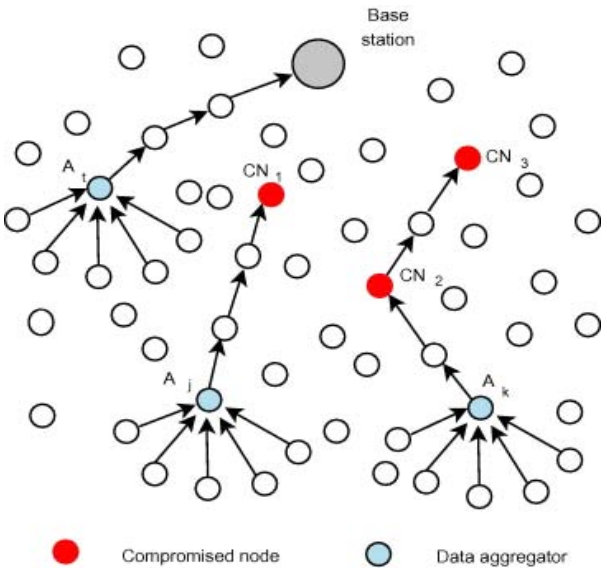

Fig. 5 : Selective Forwarding

In Wormhole attacks, the messages received in one part of the network are channeled over a low latency link, to be replayed in another part of the network (cf. Figure 6).

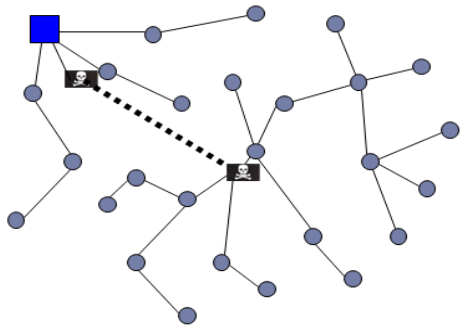

Fig. 6 : Wormhole Attack

In this attack, faraway nodes are convinced that they are neighbors, thus quickly depleting their power resources through inefficient routing. For instance, an attacker near the base station can convince nodes which are many hops away that they are close to the base through the wormhole.

HELLO' messages are broadcasted to announce their presence to neighboring nodes (cf. Figure 7). In the Hello Flood attack, the goal is to convince every node in the network that it is its neighbor, as well as advertising that it has a high quality route. This is done by the attacker using a high powered antenna. Thus, nodes that are a great distance away from the attacker will send packets to it, into oblivion, since the messages will never reach, causing confusion in the network.

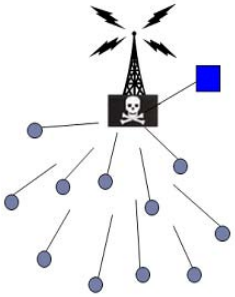

Fig. 7 : HELLO Flood Attack

Another attack is called Acknowledgement Spoofing (cf. Figure 8). The acknowledgement packet is spoofed to convince the node that a weak link is strong or a dead node is alive. Essentially, packets sent along such links will be lost. Protocols prone to this attack are those that choose the next hop based on reliability issues.

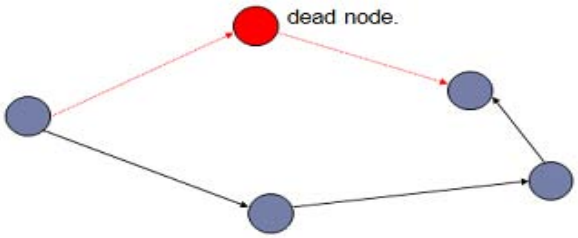

Fig. 8 : HELLO Flood Attack

In the transport layer Flooding and Desynchronisation attacks occur [7]. Flooding is similar to SYN attacks in TCP and the aim is to deplete a victim's memory resources. When many connection establishment requests are sent, the victim must allocate memory to maintain state for each connection, thus eventually overloading its memory. In desynchronisation, the attacker forges messages between sender and receiver, changing sequence numbers and control flags in the packet header. The sender and receiver could be prevented from ever exchanging messages if the attacker gets the timing right since they will continually request retransmission of previous invalid messages. This causes an infinite cycle which depletes power resources.

There are four additional attacks that will not be discussed within a particular network layer. These are Traffic Analysis attacks, Node Replication attacks, attacks against Privacy and Data Aggregation attacks [8]. There are two types of traffic analysis attacks, rate monitoring attack, in which nodes closest to the base station are observed as forwarding more packets than those farther away from the base, and time correlation attacks, in which the adversary generates an event to be sensed and observes to whom packets are sent. In both cases, the base station can be determined and disabled.

In Node Replication attacks, the ID of an existing sensor node in the WSN is copied. This can disrupt network performance through corrupted and misrouted packets leading to false sensor readings and a disconnected network. Also, if physical access is gained and cryptographic keys are copied, the replicated node can be inserted at strategic points in the network leading to manipulation or disconnection of a certain part of the network. Monitoring, eavesdropping, traffic analysis and camouflaging of adversary nodes in the network are all attacks against privacy.

Due to the computational constraints placed on individual sensor nodes, Data Aggregation [5] is used where some nodes act as aggregators and are responsible for collecting the raw data from nodes and processing/aggregating it into more usable data. This technique is vulnerable to attack since only the aggregator node needs to be targeted. A specific attack called the Stealthy attack seeks to provide incorrect results to the user without its knowledge.

IV. Countermeasures

This section looks at solutions to each of the attacks described in the previous section. Firstly, in Jamming, spread spectrum communication, at least until the jammers figure out how to block a wider part of the radio frequency band, is one solution. Code spreading is another, but it requires more design effort and power. Changing the mode of communication to infrared or optical can work but is costly. Also, the network can be made to switch to a low power cycle which it is under attack [7]. Additionally, channel hopping and blacklisting are part solutions [9]. Finally, neighboring nodes under attack could alert the base station, or could observe a change in the background noise of their neighbours and send an alert [7].

For Tampering, it is necessary to provide tamper-resistant packaging, but this is costly [7]. Camouflaging of nodes, programming nodes to erase sensitive data on capture [7] and protection and changing of keys are alternative solutions [9].

For prevention of Collision attacks, collision detection, error correcting codes – though costly, cyclic redundancy checks (CRCs) and time diversity are possible solutions [9]. For prevention of Unfairness attacks, prevent the channel from being captured for long time periods using small time frames [7]. To prevent exhaustion attacks, the problem of indefinite postponement during collisions can be solved using time division multiplexing [7]. Additionally, the link layer can ignore excessive requests without having to send radio messages by using the MAC admission control rate. Finally, protection of network ID and other data that is required for joining the network is part solution [9].

To defend against data being Spoofed, Altered or Replayed, link layer encryption and authentication must be used [7]. Also, use of different paths for resending failed messages can work [9]. For Selective Forwarding, redundancy via multi-path routing as well as regular network monitoring using source routing are adequate defenses [7], [9].

The countermeasure to the Sybil attack is verification of identities of participating nodes [7]. The first step is to have each node share a unique key with the base station. Then, two neighboring nodes can share data by encrypting data using a shared key and verifying the link between them. The base station can limit the number of legitimate nodes a compromised node can communicate with by limiting the number of verified neighbors a node can have. However, a compromised insider can still participate in the network, but should only be allowed through using compromised identities and no additional ones. Sybil attacks can also be prevented in the lower layers by regular changing of keys, resetting and physical protection of devices [9].

Since wormholes use invisible channels and the routes advertised by sinkholes are hard to verify, it is difficult to defend against Wormhole and Sinkhole attacks [7]. One solution is to use Geographic Routing Protocols which routes messages to the physical location of the base station. False links are easily discovered when the physical distance of a route exceeds the radio signal ranges of nodes. Providing tight time synchronization is another solution, but this is difficult. Finally, regular monitoring of the network and physical monitoring of field devices can be done [9].

Hello Flood attacks can be defended against by determining whether action should be taken on information received over a link through verifying the bi-directionality of that link [7]. This is known as the Needhan-Schroeder verification protocol. The base station can prevent this attack entirely by reducing the number of verified neighbours. Defense against Acknowledgement Spoofing entails authentication using encryption of all sent packets and packet headers [7]. Countermeasures for WSN attacks are shown on Table I.

Attacks	Countermeasures
Link layer	Link layer encryption. Selective forwarding, sinkhole and Sybil attacks stopped
Selective forwarding	Use multi-path routing and probabilistic-based routing.
Sybil	Unique symmetric keys. Verify identities of neighbors
Wormhole	Use private channel
Sinkhole	Verify routing metric information (such as remaining energy).
HELLO flood	Verify the bi-directionality of a link
Outsider	Authentication using a globally shared key. Selective forwarding, sinkhole and sybil attacks stopped

Table 1 : Countermeasures for WSN attacks [13]

To prevent Flooding attacks, the sender must solve a puzzle in order to get a connection. The puzzle is distributed with each connection request [7]. To flood the network, the attacker has to consume more energy; however, to get connected, legitimate nodes also have to use up additional resources. For Desynchronisation, two solutions can be used. The first is to authenticate all packets sent and all control fields, but requires expenditure of resources for legitimate nodes [7]. The second is to use different neighbours for time synchronization [9]. For Traffic Analysis attacks, regular monitoring of the network and sending of dummy packets in quiet hours are solutions [7], [9]. For Eavesdropping, defenses are using keys to protect the Data Link Protocol Data Unit and the Transport Protocol Data Unit from eavesdroppers [9].

Finally, in Stealthy attacks, data plausibility checks can be used, but requires some redundant information [8]. Additionally, multiple levels of aggregator nodes, use of deviation query where only values that deviate from a pre-defined base are transmitted, and the (CDA) concealed data aggregation approach using encryption can be used [6]. On Table II are shown security schemes for WSNs.

Security Schemes	Attacks	Major Features
JAM	DoS Attack (Jamming)	Avoidance of jammed region by using coalesced neighbour nodes
Wormhole based	DoS Attack (Jamming)	Uses wormholes to avoid jamming
TinySec, TinyPK [8]	Data and information spoofing, Message Replay Attack	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA	Data and information spoofing, Message Replay Attack	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead
SMACS – Self-Organized Medium Access Control for Sensor Networks, EARS – Eavesdrop and Register [12]	Data Link Layer protocol for WSNs [12]	Responsible for medium access, error control, multiplexing of data streams and data frame detection. Correcting of transmission errors [12]
SMECN – Small Minimum Energy Communication Network, LEACH – Low Energy Adaptive Clus-tering Hierarchy [12]	Network Layer Protocols for WSNs [12]	Responsible for intra-network operation, different type addressing routing information through the sensor network, finding the most efficient path for a packet to travel on its way to a destination [12]
Zigbee, 802.15.4 Standard [7]	Shared Keys, encryption [7]	Hardware-based symmetric keying [7]
DES – Data Encryption Standard, 3DES – triple DES, RC5, AES [8]	Use in symmetric cryptography [8]	Utilizing a shared key for both encrypting and decrypting data. [8]
LIDS – local intrusion detection system [8]	An intrusion detection architecture [8]	All LIDS within the network exchange both security data and intrusion alerts. [8]
Statistical En-Route Filtering	Information Spoofing	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution	Sybil Attack	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting Sybil entity
Bi-directional Verification, Multipath multi-base station routing	Hello Flood Attack	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security	Information or Data Spoofing	Efficient resource management, Protects the network even if part of the network is compromised
TIK	Wormhole Attack, Information or Data Spoofing	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Pre-distribution	Data and information spoofing, Attacks on information in Transit	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD	Black hole attacks	Uses geographic routing, Takes advantage of the broadcast inter-radio behaviour to watch neighbour transmissions and detect black hole attacks

Table 2 : Security Schemes for WSNs [4]

V. Conclusions

Because of these strict requirements of wireless sensor networks modern security mechanisms needs to be developed. These security solutions have to be incorporated into the network protocol and have to be adapted to suit the nature of sensor networks. Currently proposed solutions solve specific attacks and much more work has to be done to find solutions that would solve the majority of sensor network attacks. Presently research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, but there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. With advances in

technology motes may get stronger and existing solutions, though limited, will have to be upgraded to meet the new technological landscape.

Two future research topics are: (1) Exploit the availability of private key operations on sensor nodes: recent studies on public key cryptography have shown that public key operations may be practical in sensor nodes. However, private key operations are still very expensive to realize in sensor nodes. As public key cryptography can greatly ease the design of security in WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable. (2) QoS and security: performance is generally degraded with the addition of security services in WSNs. Current studies on security in WSNs focus on individual topics such as key management, secure routing, secure data aggregation, and intrusion detection. QoS and security services need to be evaluated together in WSNs. By more carefully considering the threats posed to sensor networks, applications with intrinsic security considerations become immediately realizable.

References Références Referencias

1. Lewis, F. L. 2004. Wireless Sensor Networks. In Smart Environments: Technologies, Protocols, and Applications. Ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004. Available: http://arri. uta. edu/acs/networks/WirelessSensorNetChap04.pdf
2. Stankovic, J. Wireless Sensor Networks. Chapter in Handbook of Real-Time and Embedded Systems, CRC Press, 19 pages, 2008. Available: https:// www.cs.virginia.edu/~stankovic/psfiles/wsn.pdf
3. Römer, K., Mattern, F. The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61, December 2004. Available: http://wsn. cse. wustl. edu/images/8/8c/Wsn-design04.pdf
4. Khan Pathan, A., Lee, H., &Hong, C. S. Security in Wireless Sensor Networks: Issues and Challenges, Proceedings of the 8th International Conference on Advanced Communication Technology (IEEE ICACT 2006), Volume II, 20-22 February, Phoenix Park, Korea, 2006, pp. 1043-1048. Available: http://arxiv. org/ftp/arxiv/papers/0712/0712.4169.pdf
5. Perrig, A., Stankovic, J., & Wagner, D. Security in Wireless Sensor Networks, In Communications of the ACM (CACM), Vol. 47, No. 6, June 2004. Available: http://www.cs.virginia.edu/~stankovic/ psfiles/security.pdf
6. Westhoff, D., Girao, J., & Sarma, A. Security solutions for wireless sensor networks. NEC Journal of Advanced Technology, 59(2), June 2006. Invited paper. Available: http://www.ist-ubisecsens.org/ publications/SecuritySolutionsWSN.pdf
7. Kaplantzis, S. Security Models for Wireless Sensor Networks. Supervisors Dr, N. Mani, Prof. M. Palaniswami, Prof G. Egan. CiteSeerX: 10.1.1.87.4605, 2006. Available: http://members. iinet.com.au/~souvla/transfer-final-rev.pdf
8. Walters, J.P., Liang, Z., Shi, W., & Chaudhary, V. Wireless sensor networks security: a survey, Technical Report MIST-TR-2005-007, July 2005. Available: http://www.eecis.udel.edu/~fei/reading/ 070426.wsn.security.survey.pdf
9. Kalita, H., K., Kar, A. Wireless Sensor Network Security Analysis. International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009. Available: http://airccse.org/ journal/ijngn/papers/1.pdf
10. Ameen, M., A., Jingwei, L., & Kyungsup, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems. 2012-02-01. Springer Netherlands.SN - 0148-5598, Pg 93 – 101. Vol 36. No. 1. DOI 10.1007/s10916-010-9449-4, 2012. Available: http://dx.doi.org/10.1007/s10916-010-9449-4
11. Sora, D. Security Issues in Wireless Sensor Networks. International Journal of Online Engineering (iJOE). 6(4): 26-30 (2010). ISSN: 1861-21216, 2010. Available: http://www.online-journals. org/index.php/i-joe/article/view/1466
12. Singh, S., Verma, H., K. Security For Wireless Sensor Network. International Journal on Computer Science and Engineering (IJCSE) 3(6), 2393 – 2399. 2011. Available: http://www.enggjournals.com/ ijcse/doc/IJCSE11-03-06-131.pdf
13. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE Int'l Workshop on Sensor Network Protocols and Applications, May 2003.

This page is intentionally left blank