International Journal of communication and computer Technologies, ISSN: 2278-9723
Available at http://www.ijccts.org

A Review of Secure Protocols on Wireless Network Technologies

[1]A. Sasikala, [2]K. Kumaresan
[1]PG scholar,[2]Assistant Professor, Department of Information Technology, K.S.R.College of Engineering

Received: 15-06-2015, **Revised:** 30-08-2015, **Accepted:** 06-11-2015, **Published online:** 26-12-2015

ABSTRACT

Wireless Sensor Networks (WSNs) are used in a various kind of applications in military, ecological, and health-related areas. Security is consequently important in WSNs. However, WSNs suffer from many constraints, collectively with low computation capability, small memory, limited energy resources, capable to physical capture, and the role of anxious wireless communication channels. These constraints make security in WSNs a challenge. In this paper discussed about the security requirements, security attacks and secures routing protocols in WSNs. This paper studies the security ideas of wireless sensor networks. A survey with current threats and steps is carried out, in particular, investigated the protocol layer attack on sensor networks. These issues are classified into five categories: cryptography, key management, protect the routing, protect the data aggregation, and intrusion detection. Along the way we highlight the merits and demerits of different WSN security protocols according to each of these five categories. We also list out the open security issues in each subarea and conclude with possible for progress research directions on security in WSNs.

Keywords: **Wireless Sensor Networks, Data Confidentiality, Sinkhole attack, Sybil Attack, Wi-Fi Protected Access**

1. INTRODUCTION

A wireless sensor network (WSN) contain number of nodes used for monitoring purpose which pass the information composed via the network to a main location mainly a base station. The improvement of wireless sensor networks was stimulated mainly by military applications. But nowadays WSN are used popularly in many applications similar to remote control and monitoring, healthcare management, construction safety, emergency response information, logistics and inventory management etc. Wireless Sensor Networks are heterogeneous systems containing many no of small devices called sensor nodes. These networks will consist of thousands of low cost, low power and self-organizing nodes which are extremely disseminated either inside the system or very close to it. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is associated to one (or sometimes several) sensors.

Wireless sensor networks have many applications in homeland, military security and other areas in such area many sensor networks have delegate vital jobs. Security is vital for a network which deployed in hostile environments. Most sensor networks actively supervise their surroundings and it is often easy to infer information other than the data supervised. Such undesirable information outflow often results in privacy breaches of the people in environment. Moreover the wireless communication employed by sensor networks suffers from eavesdropping and packet injection by an adversary. The security for wireless sensor networks at design time to control operation safety privacy of sensitive data and privacy for people in sensor environments. Allowing security in sensor networks is even more critical than MANETs due to the resource limitations of sensor nodes.

In first section, any organization wants to protect its sensitive data, to detect tampering of data and to limit approach to authorized individuals, several industries must also comply with an array of regulatory and industry requirements and guidelines [13]. The requirements discussed in this section are authentication, integrity, authorization, confidentiality, availability, non-repudiation and freshness.

In section 2 discuss about the security threats that can be handled using structured network security architecture, which includes changes to conventional security services such as confidentiality, integrity and authenticity to the wireless domain. Wireless networks are susceptible to which are not adequately addressed through cryptographic methods. In this

paper we mainly explain the different ISO layer attacks namely the jamming, DoS, flooding, Sybil attack, etc. In Section 3 briefly describes special secure routing protocols and its techniques have been developed for use in WSNs.

In fourth section, we discuss about the various security issues, we discusses about the security issues that arise in WSN because of its resource restrictions. We have surveyed the security issues in WSNs starting with the attacks and countermeasures in each network layer followed by the issues and solutions in cryptography, key management, secure routing, secure data aggregation, and, finally, intrusion detection.

In section 5, we discuss about the literature survey of different wireless security protocols by supporting the various technologies. Fig 1 shows architecture of wireless communication. The various available wireless technologies disagree in local usability, coverage range and performance, and in some circumstances, users must be able to apply multiple connection types and switch between them. Supporting technologies include:

Wi-Fi is a wireless local area network that changes portable computing devices to link easily to the Internet. Standardized as IEEE 802.11 a/b/g/n, Wi-Fi accesses the speeds of some types of wired Ethernet. Wi-Fi has become rule measures for access in private homes, within offices, and at public hotspots.

Cellular Data Service provides coverage within a scope of 10-15 miles from the closest cell site. Speeds have increased as technologies have developed, from original technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

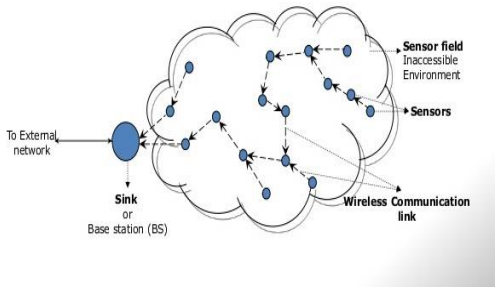

Fig. 1.Wireless Communication Architecture

Mobile Satellite Communications may be utilized where other wireless connections are unusable, such as in largely rural field or remote positions. Satellite communications are particularly significant for transportation, aviation, maritime and military use.

Wireless Technology allows services, such as long rate communications, that are insufferable or impractical to enforce with the employ of wires. The term is commonly utilized in Telecommunications Industry to denote to telecommunications systems (*e.g.,* radio transmitters and receivers, remote controls, computer networks, network terminals, *etc.*,) which employ some form of energy (*e.g.*, radio frequency (RF), infrared light, laser light, visible light, acoustic energy, *etc.*,) to transmit data without the use of wires. Information is transferred in this way over both short and long distances [1, 2].

The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Wireless technology is becoming more and more popular due to so many advantages.

2. SECURITY REQUIREMENTS

Wireless Sensor Network is dangerous to several attacks like any other conventional network, but its limited resource characteristics and unequalled application has requires some extra security requirements including the typical network requirements. The objective of security services in WSNs is to protect the information and resources from attacks and misbehaviour. Security requirements in WSNs include:

2.1 Authentication and integrity

Authentication, which controls that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node. The process of identifying an individual usually based on a username and password. In security systems, authentication is discrete from authorization, which is the process of giving individuals access to system objects based on their identity. Integrity, which ensures that a message sent from one node to another, is not modified by malicious intermediate nodes.

Only allowing data confidentiality is not enough to control the data security in WSN. As an adversary can change messages on communication or interject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication allows the truthfulness of quality of the sender. Data authentication ensures the receiver that the data has not been altered throughout the transmission.

2.2 Data Confidentiality

Confidentiality is the security of personal information. Confidentiality stands for holding a client's information between the person and the client, and not ordering others including co-workers, friends, family, etc. Confidentiality controls that a given message cannot be realized by anyone other than the hoped recipients.

Data confidentiality is one of the critical security requirements for WSN because of its application purpose (for example, military and key distribution applications). Sensor nodes transmit sensitive information, so it is necessary to control that any intruder or other contiguous network could not get confidential data intercepting the transmissions. One standard security method of allowing data confidentiality is to encrypt information and use of shared key so that only intended receivers can get the sensitive data.

2.3 Availability

Availability controls that the trusted network services are useable even in the presence of denial-of-service attacks. It is the chance that a system will work as required when required during the period of a mission. We cannot neglect the significant of availability of nodes when they are needed. For example, when WSN is used for supervising role in manufacturing system, unavailability of nodes may neglect to discover potential accidents.

Availability controls that sensor nodes are active in the network to satisfy the functionality of the network. It should be ensured that security mechanisms enforced for data confidentiality and authentication are granting the authorized nodes to enter in the serving of data or communication when their serves are required.

When sensor nodes have fixed battery power, unneeded computations may release them before their normal lifetime and make them unusable. Sometimes, distributed security protocols or mechanisms in WSN are worked by the adversaries to release the sensor nodes by its resources and makes them inaccessible for the network. Therefore, security policies should be involved so that sensor nodes do not do excess computation or do not attempt to allocate excess resources for security intention.

2.4 Non repudiation

Non repudiation, which refers that a node cannot refuse transmitting a message it, has previously transmitted. Non- repudiation is the authority that individual cannot refuse something. It denotes to the power to provide that a node to a compact or a communication cannot deny the authenticity of their signature on a message that they developed.

2.5 Freshness

Data Freshness involves that the data is recent and provide that no opponent can replay previous messages. This prevents the adversaries from obscuring the network by replaying the appropriated messages replaced between sensor nodes. To attain freshness, security protocols must be designed in such a path that they can discover duplicate packets and dispose them preventing replay attack Furthermore, as new sensors are spread and old sensors neglect, we propose that forward and backward secrecy should also be viewed.

- Forward secrecy: a sensor should not be capable to study any succeeding messages after it departs the network.
- Backward secrecy: a linking sensor should not be capable to study any previously communicated message.

The security services in WSNs are generally focused on cryptography. However, referable to the restrains in WSNs, many already existing secure algorithms are not virtual for usage.

2.6 Authorization

Authorization, which ensures that only authorized sensors, can be involved in providing information to network services. Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy. For example, human resources staff is normally authorized to access employee records and this policy

is usually formalized as access control rules in a computer system.

3. SECURITY ATTACKS

WSNs are vulnerable to several types of attacks. Allowing to the security requirements in WSNs, these attacks can be categorized:

- Attacks on secrecy and authentication: standard cryptographic techniques can assist the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.
- Attacks on network availability: attacks on accessibility are frequently denoted to as denial-of-service (DoS) attacks. DoS attacks may point any layer of a sensor network.

For securing the Wireless Sensor Networks, it is requirement to address the attacks and then take counter measures at the design time of WSN. This section gives a brief discussion about the major attacks against Wireless Sensor Network.

3.1 Physical Attack

Physical attack is also known as node capture. In this type of attack, attackers gain full control over some sensor nodes through direct physical access [16]. As the cost of sensor nodes must be kept as cheap as possible for WSN, sensor nodes with tamper proofing characteristics are impractical. This is why sensor nodes are susceptible to be physically being accessed. Physical attacks have important effects on routing and access control mechanisms of WSN. For example, acquiring key information stored on sensor node's memory establishes attacker the opportunity of unrestricted access to WSN. For executing physical attack an adversary may need technical knowledge, costly equipment and other resources. Also, most of the time physical attack needs the victim node to be murdered from the deployment area for a sure amount of time.

3.2 Attacks at Different Layer

Physical attack, adversaries execute a large number of attacks remotely. These attacks take place pretending different networking layers of WSN. This subsection identifies some of these well-known attacks

3.2.1 Physical Layer

Physical layer is responsible for real data transmission and reception, frequency selection, carrier frequency generation, signalling function and data encryption. [20]This layer also addresses the transmission media among the communicating nodes. WSN applies shared and radio based transmission medium which makes it susceptible to jamming or radio interference.

Jamming:

In physical layer, jamming is a mutual attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN. [24] Says the attacker transmits radio signal randomly with the same frequency as the sensor nodes are transmitting signals for communication. This radio signal interferes with other signal sent by a sensor node and the recipients within the range of the attacker cannot receive any message.

3.2.2 Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error check. This layer is vulnerable to data hit when more than one sender tries to send data on a single transmission distribution channel.

DoS Attack by Collision Generation:

In link year, collision is return to eject the sensor node's energy. In order to give collision, the attacker listens to the transmissions in WSN. When he finds out the initiating of a message, he sends his possess radio signal for a small amount of time to interfere with the message [16] which induces CRC error at the recipient end. Because of this attack, the receivers cannot receive the message correctly.

3.2.3 Network Layer

Network layer is answerable for routing messages from one to another node which are neighbours or may be multi hops away for example, node to ground station or node to cluster leader. The network layer for WSN is usually designed considering the power efficiency and data centric features of WSN. There are several attacks exploiting routing mechanisms in WSN. Some intimate attacks are numbered here.

Selective Forwarding:

Selective forwarding is an attack where compromised or malicious node just neglects packets of its interest and selectively forwards packets to minimize the suspicion to the neighbour nodes. The affect becomes worse when these malicious nodes are at closer to the base station [10]. Then many sensor nodes route messages by these malicious nodes. As a consequence

of this attack, a WSN may give wrong observation about the environment which pretends badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring.

Sinkhole attack:
In sinkhole attack, Fig 2 shows compromised nodes attracts a large number of traffic of surrounding neighbors by spoofing or play again an advertisement of high character route to the base station [13]. The attacker can do any malicious activity with the packets passing by the compromised node.

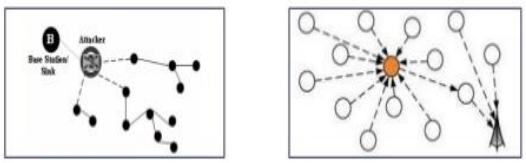

Fig. 2.Black Hole and Sinkhole

Wormhole Attack:
Wormhole is a critical attack, where the attacker finds packets at one point in the network, tunnels them through a less latency link than the network links to some other point in the network and replay packets there locally [14]. This converts the neighbor nodes of these two last points that these two distant points at either end of the tunnel are extremely near to each other. If one last point of the tunnel is at near to the base station, the wormhole tunnel can attract important amount of data traffic to interrupt the routing and operational functionality of WSN. In this case, the attack is interchangeable to sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station.

Sybil Attack:
In Sybil attack, Fig 3 shows a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has important effect in geographic routing protocols [13]. In the location based routing protocols, nodes necessarily to exchange location data with their neighbours to route the geographically addressed packets efficiently.

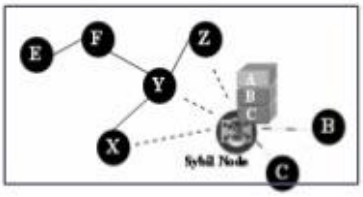

Fig. 3.Sybil Attack

Sybil attack interrupts this protocol functionality simultaneously being at more than one place. Identity verification is the key essentials for countering against Sybil attack. Dissimilar traditional networks, verification of identity in WSN cannot be acted with a single shared symmetric key and public key algorithm because of computational limitation of WSN.

3.2.4 Transport Layer

In network layer end to end connections are handled.
Flooding Attack:
According to [22] and [14], at this layer, adversaries work the protocols that hold state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to neglect its resources causing the Flooding attack. One solution against this attack is to determine the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node.

4. SECURE ROUTING PROTOCOLS

Many routing protocols have been particularly designed for WSNs. These routing protocols can be divided into three categories allowing to the network structure: flat-based routing, hierarchical-based routing, and location-based routing. In flat-based routing, all nodes are generally assigned equal roles or functionality. In hierarchical-based routing, nodes play dissimilar proposes in the network. In location-based routing, sensor node positions are used to route data in the network. Although dozens of sensor network routing protocols have been proposed in literature, few of them have been designed with security as a destination. Lacking security services in the routing protocols, WSNs are vulnerable to many kinds of attacks.
Most network layer attacks against sensor networks descend into one of the categories described above, namely:

- Spoofed, changed, or replayed routing information
- Selective forwarding
- Sinkhole
- Sybil
- Wormholes
- Hello flood attacks
- Acknowledgment spoofing

These attacks may be enforced to compromise the routing protocols in a sensor network. For example,

directed diffusion is a flat-based routing algorithm for absorbing information from a sensor network [25]. In directed diffusion, sensors evaluate events and create gradients of data in their respective neighboring nodes. The base station requests data by broadcasting interest which describes a task to be conducted by the network. The interest is diffused through the network hop by hop, and broadcasted by each node to its neighbors. As the interest is propagated throughout the network, gradients are setup to attract data satisfying the query towards the requesting node. Each sensor that receives the interest sets up a gradient for the sensor nodes from which it received the interest. This process extends till gradients are setup from the sources back to the base station. Interests initially specify a low rate of data period, but once a ground station starts receiving events it will reinforce one or more neighboring nodes in order to request higher data rate events. This process precedes recursively until it reaches the nodes generating events, causing them to generate events at a higher data rate. Paths may also be negatively reinforced. Directed diffusion is vulnerable to many kinds of attacks if authentication is not included in the protocol [18]. For example, it is easy for an adversary to add himself/herself onto the path taken by a flow of events as described in the following:

- The adversary can influence the path by spoofing positive reinforcements. After receiving and rebroadcasting an interest, an adversary could strongly reinforce the nodes to which the interest was sent while spoofing high-rate, low-latency events to the nodes from which the interest was obtained.
- The adversary can replay the interests intercepted from a logical base station and list himself/herself as a base station. All events satisfying the interest will then be sent to both the adversary and the legitimate base station.

By using the attacks above, the adversary can add him/ her onto the path and thus gain full control of the flow.

The adversary can eavesdrop, modify, and selectively forward packets of his/her choosing. He/she can drop all forwarded packets and act as a sinkhole. Further, a laptop-class adversary can exert great influence on the topology by using a wormhole attack. The adversary creates a tunnel between a node located near a base station and a node located close to where events are likely to be generated. By spoofing positive or negative reinforcements, the adversary can push data flows away from the base station and towards the nodes selected by the adversary.

Hierarchical and location based routing protocols not incorporating security services are also vulnerable to many attacks [18]. For example, location-based routing protocols such as Geographic and Energy Aware Routing (GEAR) [4] require location information to be replaced between neighbors. However, location data can be misrepresented.

Regardless of the adversary's actual location, he/she may advertise false position data to place himself/herself on the path of a known flow. Once on that path, the adversary can mount selective forwarding and Sybil attacks in the data flows. Simulations in [5] found that such attacks have great influence on the overall ratio of successfully delivered messages in the network. Secure routing in ad hoc networks is exchangeable to that in sensor networks and has been well studied in the literature [17].

However, the defences mechanisms originated for ad hoc networks cannot be directly applied to sensor networks because of the deviations between sensor and ad hoc networks talked over earlier.

Ideally, a secure routing protocol should guarantee the integrity, authentication, and availability of messages in the presence of adversaries of arbitrary power. In the presence of only outsider adversaries, it is imaginable to achieve these idealized goals. However, in the presence of compromised nodes or insider adversaries, especially those with laptop class capabilities, it is most likely that some if not all of these destinations are not fully discoverable. In this situation, the best we can hope for is graceful degradation instead of a complete compromise of the network. To achieve the above goal requires that a routing protocol degrades no faster than a rate roughly proportional to the ratio of compromised nodes to total nodes in the network [18].

A secure routing protocol depends on an appropriate key management scheme in a WSN. Before a routing protocol starts, sensor nodes should have been loaded with proper keys (e.g., the key for confidentiality, authentication, etc.). One of the fundamental security services in sensor networks is broadcast authentication, which enables the base station to broadcast authenticated data to the entire sensor network. In this section, we first discuss the broadcast authentication problem and then review several secure routing schemes.

5. SECURITY ISSUES

5.1 Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to major power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

5.2 Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to form an efficient the security mechanism, it is necessary to limit the code size of the security algorithm.

5.3 Power Limitation

Energy is the biggest constraint to wireless sensor capabilities. We presume that once sensor nodes are spread in a sensor network, they cannot be easily replaced (high operating cost) or reloaded (high cost of sensors). Hence, the battery charge taken with them to the field must be conserved to lead the life of the individual sensor node and the entire sensor network.

When enforcing a cryptographic function or protocol within a sensor node, the energy effect of the added security code must be regarded. When contributing security to a sensor node, we are concerned in the effect that security has on the lifespan of a sensor (i.e., its battery life). The additional power exhausted by sensor nodes due to security is related to the processing required for security operates (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security concerned information or overhead (e.g., initialization vectors required for encryption/decryption), and the energy wanted to store security arguments in a secure mode (e.g., cryptographic key storage).

5.4 Unreliable Communication

Surely, unreliable communication is some other threat to sensor security. The security of the network trusts hardly on a determined protocol, which is depends on communication.

5.5 Unreliable Transfer

Normally the packet-based routing of the sensor network is association and thus inherently unreliable. Packets may get damaged due to channel errors or at highly congested nodes. The outcome is lost or missing packets. Moreover, the unreliable wireless communication channels also final results in discredited packets. Higher channel error rate also forces the software developer to commit resources to error handling. More significantly, if the protocol lacks the appropriate error handling it is potential to miss critical security packets. This may include, for example, a cryptographic key.

5.6 Conflicts

Even if the channel is authentic, the communication might be unauthentic. This is preferable to the broadcast nature of the wireless sensor network. If packets assemble in the middle of transfer, struggles will occur and the transfer itself will fail. In a pushed (high density) sensor network, this can be a main trouble.

6. LITERATURE REVIEW

The KirtiRaj Bhatele, *et al.*, [11] presented hybrid security protocol for improve security using a hybrid of both symmetric and asymmetric cryptographic algorithms. The hash value of the decrypted message applying AES algorithm is calculated using MD5 algorithm. This hash value has been encrypted with dual RSA and the encrypted message of this hash value also sent to destination. At the present the reception side, hash value of decrypted plaintext is calculated with MD5 and then it is equated with the hash value of original plaintext which is calculated at the sending end for its integrity. By the way we are able to experience whether the original text being altered or not during transmission in the communication medium.

Arash Habibi Lashkari, *et al.*, [12] presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, WPA improvements such as cryptographic content integrity code or MIC, raw IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problems on WPA that happened on PSK part of algorithm. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

Gamal Selim, *et al.*, [15] explained various types of security attacks modification, fabrication, interception, brute force, maintainability and static placement of MIC. They surveyed currently available security protocols i.e. WEP, WEP2, WPA and WPA2. They also proposed a new mechanism called multiple slot system (MSS). MSS makes use of the key selector, slot selector and MIC shuffle selector. MSS uses one of four encryption algorithm RC4, RSA, Blowfish and AES.

Hyung-Woo Lee, *et al.*, [23] explained various issues and challenges in wireless sensor network. Paper explained two types of wireless security attacks – one is the attack against the security mechanisms and another is against the basic mechanisms like routing mechanism. Major attacks explained are denial of service attack, attacks on information in transit, sybil attack, hello flood attack, wormhole attack, black hole/sinkhole attack. Paper also explained the various security schemes for wireless sensor networks like wormhole based, statistical en-route filtering, random key and tinysec. Holistic opinion of security in wireless sensor networks is also explained.

Lifeng Sang, *et al.*, [6] proposed shared secret free security infrastructure for wireless networks based on two physical primitives: cooperative jamming and spatial signal enforcement. Cooperative jamming is for confidential wireless communication and spatial signal enforcement is for message authenticity. Proposed infrastructure provides confidentiality, identity authentication, message authentication, integrity, sender non-repudiation, receiver non repudiation and anonymity.

Andrew Gin, *et al.*, [7] compared the performance analysis of evolving wireless 802.11 security architecture. Paper explained wireless network security methods. Paper explained security layers like WEP shared key authentication and 40 bit encryption, WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption, WPA with EAP-TLS authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption. Effects on throughput are also discussed.

Eric Sabbah, *et al.*, [8] explained attacker motivation, vulnerabilities and opportunities currently available to hackers. Wireless sensor networks are exposed to numerous security threats that can endanger the success of the application. Paper explains that security supports in wireless network is challenging due to the limited energy, communication bandwidth and computational power. Security issues and currently

available solutions, various types of attacks like - attacks on routing and DoS attack, injecting false packets, attacks on real time requirements, attacks on the network using topological information, attacks on localization.

Floriano De Rango *et. al.*, [3] proposed static and dynamic 4 - way handshake result to deflect denial of service attack in WPA and IEEE 802.11i. Paper also explained DoS and DoS flooding attacks against IEEE 802.11i 4-way handshake. Paper also compared static versus dynamic resource oriented solutions for the 4 way handshake.

Stephen Michell, *et al.,* [9] proposed state based key hope protocol (SBKH) that provides a lightweight encryption system for battery function devices such as the sensors in a wireless sensor network as well as small office, home office (SOHO) users. State based key hope protocol implements encryption in a novel state based way so as to ensure cheap and robust security without extra overheads of encryption. Implementation of SBKH on real hardware is a challenge.

7. CONCLUSION

In this paper, we give a study on wireless sensor network, its requirements, issues, and attacks. Security is a significant requirement and refine enough to set up in different parts of WSN developing such a security mechanism and making it effective constitutes a great explore. Again, ensuring reliable security in wireless sensor network is a major issue. The proposed security schemes are based on particular network models in future though the security strategies become well-founded for each individual layer; combining all these mechanisms together for making them work in a unit will obtain a hard explore. It is observed that many organizations are currently deploying wireless networks typically to use IEEE 802.11b protocols, but technology used is not secure and still highly susceptible to active attacks and passive intrusions. Currently available security protocols like WEP, WPA and WPA2 have some advantages and disadvantages and also there are some vulnerability exists in these security protocols. Then present the literature survey on various security techniques for WSN.

REFERENCES

[1] http://csrc.nist.gov/wireless.

[2] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[3] F. De Rango, D. C. Lentini and S. Marano, Editors, “Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i”, EURASIP Journal on Wireless Communications and Networking, **(2006)** June.

[4] Y. Yu, R. Govindan, and D. Estrin, “Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks,” UCLA Computer Science Department, Tech. Rep. UCLA/CSD-TR-01-0023, May 2001.

[5] T. Leinmüller *et al.*, “Influence of Falsified Position Data on Geographic Ad-Hoc Routing,” *2nd European Wksp. Security and Privacy Ad Hoc and Sensor Networks (ESAS 2005)*, LNCS, July 2005.

[6] L. Sang and A. Arora, Editors, “A Shared Secret Free Security Infrastructure for Wireless Networks”, ACM Transactions on Autonomous and Adaptive Systems (TAAS), **(2012)** July.

[7] A.Gin and R. Hunt, Editors, “Performance Analysis of Evolving Wireless IEEE 802.11 Security Architectures”, ACM International Conference on Mobile Technology Applications and Systems, **(2008)**.

[8] E. Sabbah, A. Majeed, K. Y.-D. Kang, K. Liu and N. Abu-Ghazaleh, Editors, “An application-driven perspective on wireless sensor network security”, ACM international workshop on Quality of service & security for wireless and mobile networks, **(2006)**.

[9] S. Michell and K. Srinivasan, Editors, “State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks”, ACM international workshop on performance evaluation of wireless adhoc, sensor, and ubiquitous networks, **(2004)**.

[10] Mayank Saraogi . Security in Wireless Sensor Networks. In *ACM SenSys*, 2004.

[11] K. Bhatele, A. Sinhal and M. Pathak, Editors, “A Novel Approach to the Design of New Hybrid Security Protocol Architecture”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), **(2012)** August 23-25, Ramanathapuram.

[12] A.H. Lashkari and M. M. S. Danesh, Editors, “A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i”, IEEE International Conference on Computer

Science and Information Technology, **(2009)** August 8-11, Beijing.

[13] Stamatios and V. Kartalopoulos, Editors, "Differentiating Data security and Network Security", IEEE International Conference on Communications, **(2008)** May 19-23, Beijing.

[14] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In *IEEE Pervasive Computing*, volume 7, pages 74–81, 2008.

[15] G. Selim, H. M. E. Badawy and M. A. Salam, Editors, "New Protocol design for Wireless Networks security", IEEE International Conference on Computer Science and Information Technology (ICACT), **(2006)** Feb 20-22.

[16] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In *ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication*, page 40, Washington, DC, USA, 2006. IEEE Computer Society.

[17] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy Special Issue: Making Wireless Work*, vol. 2, no. 3, May/June 2004, pp. 28–39.

[18] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications*, May 2003, pp. 113–27.

[19] J. Hill *et al.*, "System Architecture Directions for Networked Sensors," *SIGOPS Oper. Syst. Rev.*, vol. 34, no. 5, 2000, pp. 93–104.

[20] John PaulWalters, Zhengqiang Liang,Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A survey. *Security in Distributed, Grid, and Pervasive Computing*, 2006.

[21] Khalil, S. Bagchi, and N. B. Shroff. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Comput. Netw.*, 51(13):3750–3772, 2007.

[22] A.Wood and J. Stankovic, "Denial of service in sensor networks", In *Computer*, volume 35, page 54U″ 62, 2002.

[23] H.-W. Lee, A.-S. K. Pathan and C. S. Hong, Editors, "Security in Wireless Sensor Networks: issues and challenges", International Conference on Advanced Communication Technology (ICACT), **(2006)** February 20-22, Phoenix Park.

[24] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[25] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *MobiCom '00: Proc. 6th Annual Int'l. Conf. Mobile Computing and Networking*, New York: ACM Press, 2000, pp.56–67.