Security Solutions for Classified Attacks in WSNs

Muhammad Aamir Panhwar[1†], **Sijjad Ali Khuhro**[2††], **Nasrallah Pirzada** [3††], **Kamran Ali Memon** [4††], **Deng ZhongLiang** [5], **Noor ul Ain** [6††]

[1,4,5] School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China
[2] School of Computer Science and Technology, University of Science and Technology of China, China
[3] Department of Telecommunication Engineering, Mehran University of Engineering & Technology, Jamshoro, Pakistan
[6] School of Information & Communication Engineering, Beijing University of Posts and Telecommunications Beijing, China

Summary
Wireless Sensor Networks (WSN) is an emerging technology used in different applications, and thus become an interesting field of research. Besides massive advantages, related security breaches are the matter of concerns for many researchers to propose new security solutions schemes in WSNs, protect critical applications in civilian and military areas. In the past, various cryptographic solutions are devised to overcome the vulnerable attacks on WSNs. This article reviews and analyzes different types of attacks against the WSNs application, and describes the state of art security solutions. This review aims to benefit researchers as well as manufacturers to find new research direction in WSN security.

Keywords:
WSNs, Attacks, Security, Compromised node, data confidentiality.

1. Introduction

The Research advancement of Hardware Engineering approaches and powerful software methods that's would be creates collected of several sensors which called a wireless sensor network [1] [14] [27]. Wireless Sensor Networks-WSNs Raises in terms of Groups which spatially discrete as well as dedicated sensors for observing and saving the bodily situations and these would be able to manage the composed data at a mid-point. Sensors are very active and small in size, low cost and also have medium processing and computational power [31] [19] [35], However, they are very cheap than the traditional sensors. WSNs able to measure the conditions of the environment such as wind, temperature, sound, pollution levels so on and other physical conditions. WSNs research emerged in different domain of fields, supposed as I-T systems, hardware and system of design, Networks, forensic Applications which detailed in figure no.2, a different model of programming, organization of data, security challenges and different factors [2] [25, 7]. WSNs have been high prospective in different applications development such as military objective and their surveillance [33] [38], utilize the purpose of natural disaster [5], tracking data of the patient in the biomedical field [10] [20], and for exploration of hazardous environment for sensing purpose [37]. WSNs are very useful in military networks for tracking and surveillance and it is able to give support during recognition and identification. According to our knowledge basic philosophy of sensor network is to distribute the minute sensing in the shape of devices, the goal of this distribution phenomena is able to some changes in sensing parameters as well as communication with an others device within the particular geographic areas for special resolution such as, focus to track data, surveillance, monitoring the environmental conditions and so on. Wireless sensor networks connected to each other within the very short range of links, they utilize the special type of infrastructure by forwarding the collected data to authorized entities over the base-station (BS) [2] [22, 24] [25]. According to the recent research approaches sensors can observe the temperature, the pressure within the specific area, moisture, movements of objects, sounds and more others special properties [18].

In case of intelligent nodes of sensors, which are, very low power devices and the take placed in one or more than one sensors, in the regard of, a processing, memory, an acuter, a radio, etc. Generally speaking, WSNs has no proper infrastructure because of it joined with the thousands of sensors of nodes and they work together for monitoring purpose and getting data about the proper environment. WSNs categorized in two types of families. First, one is structured and second is unstructured. In regard to structured, WSNs nodes deployed in the preplanned manners, they are very beneficial during the deployment with subordinate networks repair as well as managing cost. In unstructured, WSNs environment they are very dense collected sensor nodes. Unstructured WSNs environment more chances to failure of maintained and lack of connectivity between the participant nodes. Nodes of the sensor could be deployed in a Hoc way. After the deployment phase, the network would be able to leave unattended to delivering observing and report generation functions.

In term of security it's a very important factor during the infrastructure of WSNs, nowadays many application

Manuscript received June 5, 2019
Manuscript revised June 20, 2019

suffering because of unavailability of security within the networks and many researchers trying to provide a different kind of authenticated schemes to WSNs. Security factor in WSNs has to be complete and a very basic requirement. This kind of requirements are not enough to provide authenticity of sensitive information, but it could be explored bounded resources in every sensor node, which can maintain the sensor networks in the shape of life. Adversary inspiration, susceptibilities, and chances that are two factors, which able to provide the adversary chances to affect the wireless sensor networks. Sensor nodes would be able to expose in the risk by capturing the active adversary. Therefore, it is possible to damage sensor nodes connectivity and loss of communication channel. Many keys issues occur during the design of a proper channel of WSNs environment, so it is necessary to support the WSNs environments against these problems. WSNs need proper security in term of authentication, integrity, and confidentiality for protection against the adversaries, Moreover, the characteristic boundaries in the communication channel and for calculating, deployment phase of WSNs creates more susceptible in different attacks issues. In case of deployment nodes system its occupied large size of area and attackers have more chances to attacks on confidential data between the sensor nodes, figure no.1 shows the development of WSNs network. Adversaries are sharper they could be able to use the special kind of formula to track the sensing data between the sensor nodes. The adversary has some special target such as, to detect the secret data, to hack the all collected data by within a special network and DoS-Denial of services and assured to potential threats in the regard of privacy and security within the wireless sensor networks. During the capturing of nodes by an adversary result could occur in between active and passive, as well as physical attacks could be happened by an intellectual adversary. Moreover, during the initialize or create a setup by an adversary, it will able to collect secret information by snooping to message interchanging, even a single attack device or under the network with the support of a number of attacks devices occurs in the development of the network. In condition, if the message were encrypted the attacker would be able to capture data about network working and there state. Although applications of hardware and software development might point out this kind of security problems, however, development of new technologies in the recent century they facing many security challenges issues in wireless sensor networks application during the hardware and software level approach.

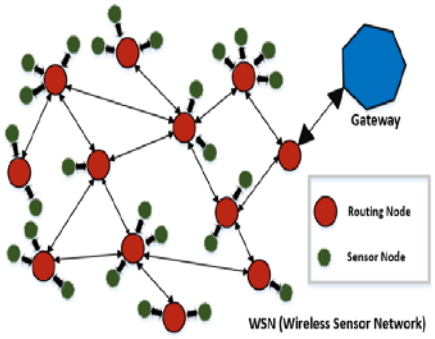

Fig. 1 WSN environment

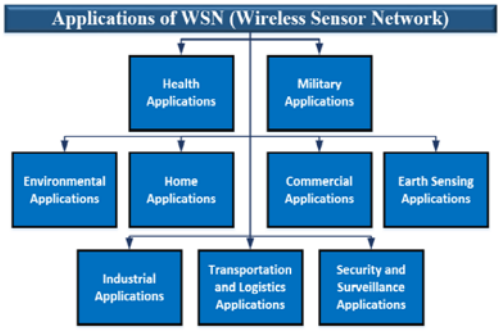

Fig. 2 Application of WSNs

Structure of our paper follows as 1. We discussed the background study of wireless sensor networks. 2. about the architecture of WSNs and sensor components. 3. Classification of attacks 4. Security solutions against the WSNs 5. Conclusion of the paper.

2. Architecture of Wireless Sensor Node

A sensor node depends on four basic components such as sensing component, processing component, radio transceiver component, power source component. These four components detailed under figure.3. Sensor nodes also depend on more additional components. Sensing component depends on more two sub-components called sensor and analogue, which directed to the digital converters. Sensors are able to create analogue signals, which can be converted to the digital signal, and then able to feed in the processing component. Generally talking, processing component connected with the storage component and it can be organized the functions that create the node of sensors as a collaborator to the sensor nodes for assigning the sensing responsibilities. The duty of the transceiver component to joints nodes within the network environments. We analysis power component is a very

important part of the WSNs environment because it would be able to supported by the solar cells.

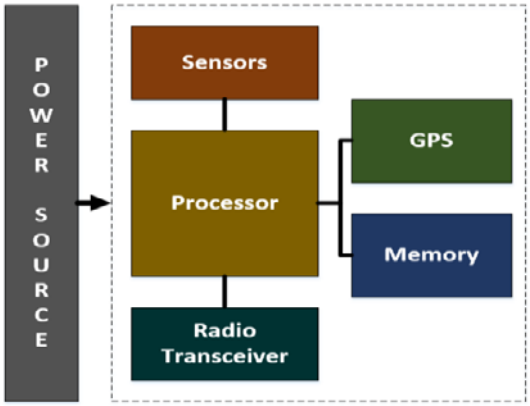

Fig. 3 Components of node

Working flow diagram of sense is given in figure no.4. Components design approach provides the flexibility in Verities in WSNs applications. Suppose as, it depends on the sensor node during the deployment phase, signal components are able to be reprogramming or swapped. That is permitted in a wide range of verity in different sensors and they would be able to use sensing node values. In the same way, the radio link could be exchanged according to the requirement of application as well as the need for a bidirectional communication system.

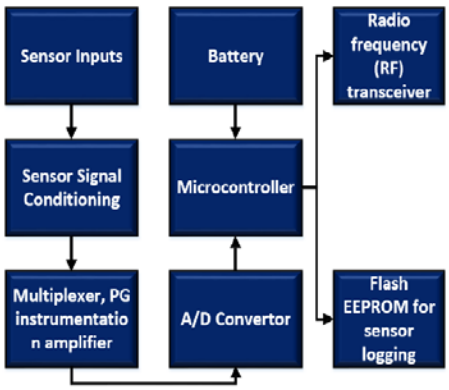

Fig. 4 Workflow of sensor

3. Classification of Attacks in WSNs

A wide area sensor network contains large amount sensor nodes why can say in thousands, its possibilities they could be dispersed over a large range of scale. However, WSNs nodes are too much small with regard to communication as well as calculating competences and supply power and batteries a matter. Such kind of problems causes to attacks on WSNs nodes and adversaries have many possibilities of ways to attack nodes and hack secret data so easily. Hereunder we classified two major attacks and sub attacks.

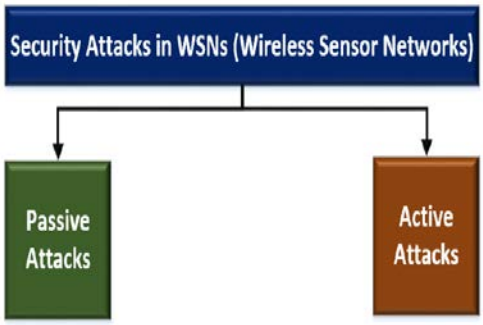

Fig. 5 The main type of attacks

3.1 Passive Attacks

It has tried to learn or create use of information from the system but it is not able to effect the system resources [17]. The attacker just can listen to communication between the medium. These attacks could take path earliest preparations, beforehand the active attacks. Simply we could say this attack in contradiction of privacy.

3.1.1 Attack on Traffic Analysis

In an attack messages could be transmitted over the network that is susceptible, however, these messages are in encrypted form. There could be a big possibility an adversary can analysis the multiple patterns of the proper communication channel. More chances sensors activities could be exposing very easily and network communication will be damaged so easily.

3.1.2 Eavesdropping/Snooping Attack

This attack is very easy violating the privacy, it could be able to detect the secret information, and the adversary would able to learn the pattern of contents within the communication. During the configuration of a wireless sensor network, it's able to compromises through theoretical information against the location of the server. This attack behaves more effect against privacy.

3.2 Active Attacks

This attack able to modify messages and real-time data streaming or able to create the wrong information in the communication channel of WSN. An intruder could be able to recurrence the basic information streams, attackers could change the communication messages, or he/she could be able to eliminate a special part of secret data, which can be

a most important part of data during the communication channel.

3.2.1 Denial of Service-Attack

This attack occurs during the failure of nodes or malicious function [4] [36]. The easiest denial of service attempts to use the obtainable resources to target sensor node, by the support of additional needless packets and would able to protect valid networks operators to retrieving facilities, which they are permitted. This attack has multiple types and it could be performed in different layers of the wireless sensor network. At the physical layer, these attacks would cause overcrowding and interfering.

3.2.2 Sybil Attack

Different cases, sensor strength essential to working together to achieve the task, they could use the sharing the sub-task and redundancy of data. In this situation, the node could fictitious more than one node by utilizing the identities against genuine nodes. This kind of attack where node furnaces the identities of one or more than one called a Sybil attack [9] [21]. Sybil attack attempt to down the reliability of the information, this attack could be executed for hacking the dispersed storage, for routing purpose, information combination, voting, for reasonable distribution and naughtiness detection.

3.2.3 Black hole or Sinkhole Attack

This kind of Attack, a malicious node behaves as a sinkhole attack [6]. This attack detects all traffic over sensor networks. Particularly this occurs in the flood-constructed protocol. In this attack, adversary able to listen to requests very silent way for the purpose of routes and then he/she response the targeted nodes, then he follows the very short level of distance to the base station. Here adversary claims that he/she is a real node instead of a fake node, it would be able to change true information between the sensor nodes [23].

3.2.4 Hello flood Attack

This attack introduced by [15]. Attacker utilizes packets as an armament to persuade the Sensor in WSN. The attacker has the ability to send high radio transmission range to deliver hello packets nodes to the number of sensor nodes and disperse within the large range of sensor nodes, and real participant sensors feel that's it's our participant instead of a fake participant.

3.2.5 Wormhole Attack

This type of attack called a critical attack [11]. The adversary would able to try store records of multiple packets or bit at a proper location within the network and connected to another location [16]. This attack is a very noteworthy treat within the wireless sensor networks. Since this attack could not compromise within a sensor over a network, this attack would be performed although a starting point when the sensor will start for the communication purpose to each other's and getting information.

3.2.6 Masquerade Attack

This attack tries to attempt utilization of false identification to achieve the illegal entrée to any computer. The attacker will act as an unlicensed system to achieve free access and it could increase high rights instead of approving [32]. Typically, this attack another type of active attack, suppose as, certification arrangement could be achieved, and the dishonest person could get all access to the information in an illegal way.

3.2.7 Reply Attack

This attack is a family attack of the network, in this attack adversary could detect the broadcast data and is able to create delay time as well as repeated data [34, 8]. This can be carried out by an attacker or inventor that could disturb the data between the transmission medium.

3.2.8 Selective forwarding Attack

Time and secure communication is an essential part of within the network. In this type of attack, effected system by an adversary would be able to act as usual systems and it can drop targeted packets. In this attack, the targeted dropped node could be haphazard [30].

3.2.9 Node Replication Attack

In this attack, an adversary creates an easily reasonable node and he /she apply some special kind of trick between the networks and its try to claim them he/she is authenticated node [39]. This attack is very difficult to catch without the monitoring of center basis.

3.2.10 Rushing Attack

This attack we can say a modern threat in the denial of service when it has been applied in contradiction of previous routing practice within the network. An attacker able to allocate the fake messages to real messages and that can arrive later [12].

3.2.11 Attack on Modification of Messages

This attack able to attempt the function of modification or deletion of contents over networks within the proper communication. Adversary able to separate some real part of the information and it is providing the delay time during

the transferred its effect it causes to be damage of network [3].

4. Security Solutions in WSNs

WSNs applications have been the auspicious solution for security purpose as well as concern with a key. However, Research determinations have been built with cryptography, management of key, the purpose for secure routing, the security of data and accumulation, interruption and recognition in WSNs. Still, have some challenges that's could be noticed. 1: Collections of proper cryptography approaches which be subject to processing abilities of nodes of the sensor. Identify that there would be no unique clarification for each WSNs. 2: Sensor, which is classified based on limitations on energy, computing competencies, bandwidth, and memory as well as for communication channel. For designing the Wireless sensor networks these classified points must be gratifying .3: most of the current protocols claimed to be a node of sensor and base station of the sensor are in a stationary position, conversely, it's could depend on the Variety of situations, suppose as, battlefield environments, wherever the base station and probably the sensor required to be movable.

A. Cryptography Concept in WSNs

In the field of cryptography world encryption and decryption methods design for the classical wired networks, which are not suitable to be functional for WSNs. Although, WSNs based on the very small tiny sensor nodes and they are suffering because of the shortage processing system, memory, battery power [26] [13] [28]. For applying the encryption schemes its need to require additional bits for transmission. Therefore, additional memory, battery power, and processing them all are significant resources against the sensors life. When we use to apply such kind of encryption techniques, it could able to increase delay and loss of packet in WSNs [29].

B. Key Management Technique

Key management has been stated to the organization of cryptographic keys in regard of the cryptosystem. Its working based on, distribution and exchange keys as in a secure manner. This technique support to the cryptographic protocols for design purpose and it follows the proper methods within multiple protocols, especially in WSNs environment. Key management has a vital role especially in sensor node that is allocating secure key within the sensor nodes; here are some fundamental principles, which follow as:

1. **Key Redistribution scheme:** this process refers to the generation of keys and installment of keys within the different nodes of sensors.
2. **Key establishment/ key exchange scheme:** in this scheme keys could be exchanged between the two parties, simply we can say any pair of nodes or a group of different nodes create a secure pathway.
3. **Addition and elimination of node/member:** In the regard of adding member/node in a network, the additional node could be able to add for creating the secure path within the sensor network for another's secure nodes. During the elimination of node/member from a network, then it could not be able to take part again during the sensor network.

Key revocation scheme: this key helps us for re-issuing new key which never been used for cooperated with nodes. Especially there are main two types of key management.

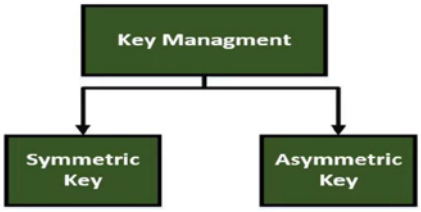

Fig. 6 Types of key management

5 **Symmetric key:** In this section, only one key could be preferred to authenticate with sensor node deployment. In Redistribution, scheme plays a vital role in sensor applications. This key likely to used mathematically operations, because of this it provides the benefit of very less computational power, it also supports to utilize very less battery power.

6 **Asymmetric key:** In this section, we can use two different keys, such as a private and public key for the purpose of encryption and decryption process. These both keys follow mathematically operation for the purpose of cooperation and during exchange keys process. This type of key opposite to the symmetric keys and this key is not suitable for WSNs applications.

C. Trusted server Scheme-TSS

This types of schemes are determined by the trusted manner and well as protected server, suppose as, key for a base station in between the nodes of agreement. Here sever could be

Preserved as the key generation center-KGC. We take a simple example, assume that two sensors want to create a secure communication channel. In this typical case, the symmetric key could be generated for every sensor node

within the WSN environments beforehand placement and fixed in every sensor nodes of memory. This placement key could be used within the two sensors to ensure the authentication between them to head the base station. After base station would be able to generate the link key or we can say session key to broadcast in a secure manner for two sensor nodes through single or multi-hops. In the KGC scheme, the base station is a very particular selection for the server.

D. Secure Key Redistribution Schemes

In these schemes, key information could be shared between every sensor nodes during the deployment phase of the sensor. Recently researchers claim that secure key Redistribution schemes are encouraging in the field of theoretical schemes.

E. PUK-Cryptography Scheme

Public key-PUK cryptography schemes techniques are very expensive for tiny sensor nodes since it's typically RSA algorithms which necessitate for high computation and this is not fit for small sensor nodes.

F. Secure routing Scheme

This is the basic functionality of WSNs environment because of its transport the information to the base stations and later it's perforce the processing of data. Although, routing is very critical functionality in WSNs. A lot of routing protocol proposed by researchers for sensor applications, Moreover, former research direction that was focused on efficiency and effectiveness of sensor networks of information broadcastings, and researchers don't focus to the security side of sensor networks and some design issue of the network in the sense of routing protocols. Deeply study and experimental work in [15] mentioned about security at the stage of design in the best way provided for routing protocol.

G. Discovery of Secure Location

As declared previous, the location of the sensor has been played a very important role in different kind of sensor applications, as we mentioned in the introduction section. Without, protection of such application adversary could easily detect the node of the location he could apply different types of attacks on such node. Suppose as the adversary can delivery wrong reference of location and he/she able to responding the real packets stopped in multiple locations. Adversary able to cooperate with an authenticated node and he would be able to send wicked references of location. Here two types of technique deal with the adversary in the regard of location discovery in WSNs, which based on MMSE-minimum mean square estimation and voting-based location estimation-VBLE to prevent the wrong location references.

H. Protected Group Management

The in-networking function of the unused data is applied in WSNs by distributing the network into a very small size of groups and examining the information combined to the group leader. In this situation, the group leader has a responsibility to confirm the data it has come from others node or not. For this technique, we need to require group key management. In adding or deleting of nodes from the group leads to more problems. In such kind of situations, we need secure protocols to control this problem.
In our proposed work, we also compared some security protocols with different parameters. Such as centralized/decentralized, energy and simulation parameters. Which are detailed in Table.1

Table 1. Proposed Results about Security based Routing Mechanism in WSNs application

Proposed work	***Cryptography Approaches***	***Centralized/Decentralized***	***Energy Consumption***	***Simulation /Results***	***Remarks***
Kyung Jun Choi [40]	Symmetric algorithms	n/a	Measured	Applied	Block & stream cipher
N. Fournel [41]	symmetric Algorithms	n/a	Measured	Applied	Block & stream cipher
M. Healy [42]	Symmetric algorithms	n/a	Measured	Applied	Block & stream cipher
YW law [43]	Symmetric algorithms	n/a	Measured	Applied	Block & stream cipher
M. Passing [44]	Symmetric algorithms	n/a	Measured	Applied	Block & stream cipher
L. Batina [45]	Asymmetric Algorithms	n/a	measured	applied, n/a , applied	Assessment presented
G Gaubatz [46]	Asymmetric Algorithms	n/a	measured	applied, n/a, applied	Assessment presented
A Liu [47]	Asymmetric Algorithms	n/a	measured	applied, na, applied	Assessment presented

M .Pugliese [48]	Hybrid	n/a	Measured	--------	Assessment presented
R. Riaz [49]	Hybrid	n/a	Measured	--------	Assessment presented
C. Castelluccia [50]	Data Accumulation	n/a	Measured	Both	----------
P. Wang [51]	Data Accumulation	n/a	Measured	Both	----------
A. Ali [52]	Secure Routing method	Decentralized, -----, -------	Measured	Both	----------
IA. Khan [53]	Secure Routing method	Decentralized,-----, -------	Measured	Both	----------
D. Xiao [54]	Secure Routing method	Decentralized,-----, -------	Measured	Both	----------

5. Conclusion and Future direction

As the growing fast development of sensors applications, these applications need the support of security because thousands of sensors deployed in a wide range of area, it makes sense that there is communication process of data between the sensors nodes would unsecure, and an attacker very easily could attack on confidential data. However, our survey article provides all answers against the problems. We classified different types of attacks on wireless sensors applications and discussed security solutions in the state of art, our article could be beneficial for security experts of WSNs they can use our security proposed techniques for the better improvement of security in WSNs. However, we are working on this article in extended version.

The straightforward domains and challenging development within the environment of WSNs could make a Networks security for those schemes could be highly challenging than conservative networks. Nevertheless, much of properties against WSNs could help address the Challenges for creating more secure networks. Initially, we all must have opportunities to make a model for safety solutions against the systems for the beginning. Although this kind of requirement is earlier part of the research for that system. Secondly, most parts of applications are expected in Addition to the installation of WSNs within the management domain, for the abridging the threat modulation. Third, it could be possible to exploit dismissal, scale point, physical features against environmental solutions. For suppose, we made a plan to create a WSNs environment, so we can endure operating. Although, less quantity of sensors portion could be compromised. We have opportunities for usage-terminated sensors to protecting the classified attacks. However, the feature of WSNs could permit the original fortifications not presentable in conservative networks.

Acknowledgment

This research work jointly supported by national natural science foundation of China under fund no # 61572454, 61562453, and 61520106007, And State Key Laboratory Intelligent Communication, Navigation and Micro-Nano System, Beijing University of Posts and Communications.

The research reported in this paper has been financially supported by the National High Technology 863 Program of China (No.2015AA124103) and by the National Key R&D Program no 2016YFB05502001. The authors are thankful for the financial support and guidance and assistance provided by the national natural science foundation of China and State Key Laboratory Intelligent Communication, Navigation and Micro-Nano System, BUPT.

References

[1] I. F. AKYILDIZ, W. SU, Y. SANKARASUBRAMANIAM and E. CAYIRCI, A survey on sensor networks, IEEE communications magazine, 40 (2002), pp. 102-114.

[2] I. F. AKYILDIZ, W. SU, Y. SANKARASUBRAMANIAM and E. CAYIRCI, Wireless sensor networks: a survey, Computer networks, 38 (2002), pp. 393-422.

[3] M. A. BEDDOE and K. GURUSWAMY, Modification of messages for analyzing the security of communication protocols and channels, Google Patents, 2013.

[4] W. BLACKERT, D. GREGG, A. CASTNER, E. KYLE, R. HOM, and R. JOKERST, Analyzing interaction between distributed denial of service attacks and mitigation technologies, DARPA information survivability conference and exposition, 2003. Proceedings, IEEE, 2003, pp. 26-36.

[5] M. CASTILLO-EFFER, D. H. QUINTELA, W. MORENO, R. JORDAN, and W. WESTHOFF, Wireless sensor networks for flash-flood alerting, Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on, IEEE, 2004, pp. 142-146.

[6] B. J. CULPEPPER and H. C. TSENG, Sinkhole intrusion indicators in DSR MANETs, Broadband Networks, 2004. BroadNets 2004. Proceedings. First International Conference on, IEEE, 2004, pp. 681-688.

[7] S. DAI, X. JING and L. LI, Research and analysis on routing protocols for wireless sensor networks, Communications, Circuits and Systems, 2005. Proceedings. 2005 International Conference on, IEEE, 2005, pp. 407-411.

[8] M. L. DAS, Two-factor user authentication in wireless sensor networks, IEEE transactions on wireless communications, 8 (2009), pp. 1086-1090.

[9] J. R. DOUCEUR, The sybil attack, International workshop on peer-to-peer systems, Springer, 2002, pp. 251-260.

[10] T. GAO, D. GREENSPAN, M. WELSH, R. R. JUANG and A. ALM, Vital signs monitoring and patient tracking over a wireless network, Engineering in Medicine and Biology

Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the, IEEE, 2006, pp. 102-105.

[11] Y.-C. HU, A. PERRIG and D. B. JOHNSON, Packet leashes: a defense against wormhole attacks in wireless networks, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, IEEE, 2003, pp. 1976-1986.

[12] Y.-C. HU, A. PERRIG, and D. B. JOHNSON, Rushing attacks and defense in wireless ad hoc network routing protocols, Proceedings of the 2nd ACM workshop on Wireless security, ACM, 2003, pp. 30-40.

[13] G. JOLLY, P. KOKATE, and M. YOUNIS, A low-energy key management protocol for wireless sensor networks, null, IEEE, 2003, pp. 335.

[14] J. M. KAHN, R. H. KATZ, and K. S. PISTER, Next century challenges: mobile networking for "Smart Dust", Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, ACM, 1999, pp. 271-278.

[15] C. KARLOF and D. WAGNER, Secure routing in wireless sensor networks: Attacks and countermeasures, Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, IEEE, 2003, pp. 113-127.

[16] I. KHALIL, S. BAGCHI and N. B. SHROFF, LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks, Dependable Systems, and Networks, 2005. DSN 2005. Proceedings. International Conference on, IEEE, 2005, pp. 612-621.

[17] S. KHAN, N. MAST, K.-K. LOO and A. SILAHUDDIN, Passive security threats and consequences in IEEE 802.11 wireless mesh networks, 2; 3 (2008).

[18] S. LALAR, Security in Wireless Sensor Networks: Issues and Security Mechanisms, (2014).

[19] F. L. LEWIS, Wireless sensor networks, Smart environments: technologies, protocols, and applications (2004), pp. 11-46.

[20] K. LORINCZ, D. J. MALAN, T. R. FULFORD-JONES, A. NAWOJ, A. CLAVEL, V. SHNAYDER, G. MAINLAND, M. WELSH and S. MOULTON, Sensor networks for emergency response: challenges and opportunities, IEEE pervasive Computing (2004), pp. 16-23.

[21] V. MANJULA and C. CHELLAPPAN, The replication attack in wireless sensor networks: Analysis and defenses, International Conference on Computer Science and Information Technology, Springer, 2011, pp. 169-178.

[22] A. NETWORK and Z. TAFA, Ubiquitous Sensor Networks, Computer Communications and Networks, Springer, pp. 267.

[23] E. C. NGAI, J. LIU, and M. R. LYU, On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, ICC, Citeseer, 2006, pp. 3383-3389.

[24] D. G. PADMAVATHI and M. SHANMUGAPRIYA, A survey of attacks, security mechanisms and challenges in wireless sensor networks, arXiv preprint arXiv:0909.0576 (2009).

[25] A. PERRIG, J. STANKOVIC and D. WAGNER, Security in wireless sensor networks, Communications of the ACM, 47 (2004), pp. 53-57.

[26] A. PERRIG, R. SZEWCZYK, J. D. TYGAR, V. WEN, and D. E. CULLER, SPINS Security protocols for sensor networks, Wireless networks, 8 (2002), pp. 521-534.

[27] G. J. POTTIE and W. J. KAISER, Wireless integrated network sensors, Communications of the ACM, 43 (2000), pp. 51-58.

[28] J. M. RABAEY, J. AMMER, T. KARALAR, S. LI, B. OTIS, M. SHEETS and T. TUAN, PicoRadios for wireless sensor networks: the next challenge in ultra-low power design, Solid-State Circuits Conference, 2002. Digest of Technical Papers. ISSCC. 2002 IEEE International, IEEE, 2002, pp. 200-201.

[29] M. SALEH and I. KHATIB, Throughput analysis of WEP security in ad hoc sensor networks, Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September, Citeseer, 2005, pp. 26-28.

[30] P. SHARMA, M. SALUJA, and K. K. SALUJA, A review of selective forwarding attacks in wireless sensor networks, International Journal of Advanced Smart Sensor Network Systems, 2 (2012), pp. 37-42.

[31] E. SHI and A. PERRIG, Designing secure sensor networks, IEEE Wireless Communications, 11 (2004), pp. 38-43.

[32] Y.-S. SHIU, S. Y. CHANG, H.-C. WU, S. C.-H. HUANG and H.-H. CHEN, Physical layer security in wireless networks: A tutorial, IEEE Wireless Communications, 18 (2011).

[33] G. SIMON, M. MARÓTI, Á. LÉDECZI, G. BALOGH, B. KUSY, A. NÁDAS, G. PAP, J. SALLAI, and K. FRAMPTON, Sensor network-based countersniper system, Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM, 2004, pp. 1-12.

[34] P. SYVERSON, A taxonomy of replay attacks [cryptographic protocols], Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, IEEE, 1994, pp. 187-191.

[35] R. VERDONE, S. PALAZZO, and M. ZORZI, Wireless sensor networks, 5th European Conference, EWSN 2008, Bologna, Italy, January 30-February 1, 2008, Proceedings, Springer, 2008.

[36] B.-T. WANG and H. SCHULZRINNE, An IP traceback mechanism for reflective DoS attacks, Electrical, and Computer Engineering, 2004. Canadian Conference on, IEEE, 2004, pp. 901-904.

[37] G. WERNER-ALLEN, K. LORINCZ, M. RUIZ, O. MARCILLO, J. JOHNSON, J. LEES, and M. WELSH, Deploying a wireless sensor network on an active volcano, IEEE internet computing, 10 (2006), pp. 18-25.

[38] J. YICK, B. MUKHERJEE and D. GHOSAL, Analysis of a prediction-based mobility adaptive tracking algorithm, Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on, IEEE, 2005, pp. 753-760.

[39] W. T. ZHU, J. ZHOU, R. H. DENG and F. BAO, Detecting node replication attacks in wireless sensor networks: a survey, Journal of Network and Computer Applications, 35 (2012), pp. 1022-1034.

[40] Choi, K.J. and J.-I. Song. Investigation of feasible cryptographic algorithms for wireless sensor network. in

Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. 2006. IEEE.

[41] Fournel, N., M. Minier, and S. Ubéda. Survey and benchmark of stream ciphers for wireless sensor networks. in IFIP International Workshop on Information Security Theory and Practices. 2007. Springer.

[42] Healy, M., T. Newe, and E. Lewis, Analysis of hardware encryption versus software encryption on wireless sensor network motes, in Smart Sensors and Sensing Technology. 2008, Springer. p. 3-14.

[43] Law, Y.W., J. Doumen, and P. Hartel, Survey and benchmark of block ciphers for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 2006. 2(1): p. 65-93.

[44] Passing, M. and F. Dressler. Experimental performance evaluation of cryptographic algorithms on sensor nodes. in Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on. 2006. IEEE.

[45] Batina, L., et al. Low-cost elliptic curve cryptography for wireless sensor networks. in European Workshop on Security in Ad-hoc and Sensor Networks. 2006. Springer.

[46] Gaubatz, G., J.-P. Kaps, and B. Sunar. Public key cryptography in sensor networks—revisited. in European Workshop on Security in Ad-Hoc and Sensor Networks. 2004. Springer.

[47] Gaubatz, G., et al. State of the art in ultra-low power public key cryptography for wireless sensor networks. in Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on. 2005. IEEE.

[48] Liu, A. and P. Ning. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. in Proceedings of the 7th international conference on Information processing in sensor networks. 2008. IEEE Computer Society.

[49] Pugliese, M. and F. Santucci. Pair-wise network topology authenticated hybrid cryptographic keys for Wireless Sensor Networks using vector algebra. in 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS). 2008. IEEE.

[50] Riaz, R., et al., A unified security framework with three key management schemes for wireless sensor networks. Computer Communications, 2008. 31(18): p. 4269-4280.

[51] Castelluccia, C., et al., Efficient and provably secure aggregation of encrypted data in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 2009. 5(3): p. 20.

[52] Wang, P., et al., Joint data aggregation and encryption using Slepian‐Wolf coding for clustered wireless sensor networks. Wireless Communications and Mobile Computing, 2010. 10(4): p. 573-583.

[53] Ali, A. and N. Fisal. Security enhancement for real-time routing protocol in wireless sensor networks. in 5th IFIP International Conference on Wireless and Optical Communications Networks, WOCN. 2008.

[54] Khan, I.A., et al., Application-based Classification and Comparison of Secure Routing Protocols in Wireless sensor Networks. SmartCR, 2015. 5(3): p. 209-22