UOIuBIH
ORSinBIH
Operations Research Society in
Bosnia and Herzegovina

Southeast Europe Journal of Soft Computing
Available online: http://scjournal.ius.edu.ba

IUS Soft Computing
Research Group

A Survey On Security In Wireless Sensor Network

Faris Fazlić[1], Seyed Ali Hashemi[1], Ahmed Aletić[1],
Ali Abd Almisreb[1,] Syamimi Mohd Norzeli[2], Norashidah Md Din[2]

[1]Faculty of Engineering and Natural Sciences,
International University of Sarajevo,
Hrasnicka cesta 15, Ilidža 71210 Sarajevo,
Bosnia and Herzegovina
alimes96@yahoo.com

[2]Institute of Energy Infrastructure,
UNITEN Kajang, Selangor 43000,
Malaysia

Article Info

Article history:

Article received on 13 January 2019
Received in revised form 25 February2019

Keywords:

wireless sensor network, security, privacy, security management attacks, protocols, architectures

Abstract

With the global use of wireless sensor network technology in different fields and for different purposes such as health care monitoring, earth sensing, air pollution monitoring, military operations monitoring or surveillance system monitoring, a problem arises. Problem that could negatively impact previously started activities and observations if not handled in a right way. Authors of this paper discuss various vulnerabilities and security threads in different applications of WSN in the real world, such as intrusion, node capture attack, black hole attack or selective forwarding attack. Potential countermeasures are proposed formatted as protocols or architectures for secure transfer of data between friendly nodes, compromises on security measures with the goal of achieving secure and reliable connection. This paper could be used as a general representation of WSN security issue with which WSN engineers are faced on a daily basis.

1. INTRODUCTION

Nowadays, the vast majority of real-world applications and challenges favor the usage of “Wireless Sensor Networks” primarily because they are more cost-effective and efficient compared to alternative approaches. This sole characteristic of wireless sensor networks grants them the capability to deploy sensor vectors under various circumstances in military and civilian applications. Nonetheless, they do suffer from a number of shortcomings as well. Most notably, imposed resource limitations and constraints, as a result of lack of data storage and power. As a result, this carries the potential to introduce major impedances when we intend to implement prevalent computer security approaches in wireless sensor networks. There are numerous attacks to exploit unreliable communication channels, one of which being “physical attacks” which have proved to have an influential mark on the performance of wireless sensor networks. Although being advantageous in old machines and being the preferred industrial option (due to their cost-effectiveness), researchers are keen to find ways to cope with security challenges while preserving the distinguished traits of wireless sensor networks.

In order to immerse in topic such as this one. Filed which shows advancements every year or so, it was needed to thoroughly dive into previous papers related to the topic of sensors, wireless sensor networks and finally wireless sensor network security. Since this field is rapidly growing in its application in solving real world problems and threats it was also needed to check upon previous surveys done on this topic, since survey depict current industry attitude towards WSN its application and security. It was managed to find different approach and understanding regarding IDS, authors of one paper presents evidences of low ability and powerfulness of WSN devices and therefor pays more attention to different security options while most of the paper show strong interest towards IDS and its implementation.

2. Discussion

Private information could be addressed by and unauthorized party and with the present of intruder inside a network, it could lead to fail of response and data interchange. Take for instance Smart Grid power system which enables use of electricity for households and companies, given that the system is in broad use with the discontinuation of data flow many individuals as well as many businesses would be harmed which could have impact of one countries economy or perhaps could lead to global economic crises. Intrusion which is later discussed in the paper represent a huge problem however it is not the only one. Most common problem with wireless sensor devices inside a WSN is signal interference or jamming. Important aspects of WSN should be taken in consideration Secrecy and Integrity, make nodes secure so that neighboring or any unauthorized nodes cannot access data aimed to that specific node and ability to preserve initial data form. Last but not least Availability, property that makes single node and WSN in general available and fully functional even when system is under attack of any kind [1].

Hiding information data and encrypting solves one issue however many more arise. Current user authentication schema requires user to register on sensor's gateway, login and then authenticate to access WSN data. System is still not resistant to replay or forgery attacks, intercepting nodes login data and using it for modifying data shared among network nodes. Proposed, enhanced security schema achieves stated requests and also improves password sharing [2].

Confidentiality assuring that data is not viewed by anyone except by the one whom it is intended, integrity of data or assuring that data after traveling through the network stays the same format and sequence and availability of server are popular security theses that should be met when implementing WSN security. Complex and advanced secure mechanisms such us RSA key encryption are not that easily feasible inside sensors of this kind since sensors in WSN are design of low power and capacity, therefore asked requirements may be compromised [3].

Transporting unwanted unauthorized traffic, over long distances could be burden for these already miniature devices. DTN or Delay Tolerant Network architecture proposes validation of data at each its hop through network to solve previously state problems. This idea could also make DOS attack harder to execute [4].

Because of the small nature of these devices many issues arose. To begin with common medium for intercommunication is broadcast, which possess an issue considering today's wide application of WSN from manufacturing to transportation, military and medicine. Broadcast could be easily eavesdropped and intercepted or even its content could be changed. Adversary may constantly use services of sensors with the goal of draining its battery and finally deprave WSN of a node member or in the long run whole WSN. Solutions for previously mentioned problems could be found in different protocols. SNEP, Sensor Network Security Protocol, prevents eavesdropping, has low number of overhead bits, offers data authentication and replay protection [5]. The vulnerability and security mechanism required, recovery and reliability mechanism are greatly influenced by the field of practical WSN application [6]. WSN sensors, sometimes called moats together with its networks encouraged future research in fields of routing, protocols, error handling, miniaturization and energy efficiency, to solve problems of importance for businesses as well as general humanity problems e.g., earthquakes, floods, wildfires [7].

One non-technical vulnerability of WSN devices, not often considered, are its physical weaknesses. These devices are most often made for inaccessible terrains and therefore are disposable and made cheap, with that consideration in mind these devices are easy to sabotage in normal, everyday life. Regarding software part of WSN, decentralized Intrusion Detection System could identify and notify about malicious changes inside specific network. To construct appropriate IDS following rules need to be followed. A failure should be raised on different occasions [8]. In contrast to firm belief of IDS inside WSNs authors here [9] are of strong belief that IDS cannot be applied on sensor networks due to simple nature of sensor devices, their weakness and low capabilities. Authors propose simple changes which could help but not replace IDS, with the introduction of watchdogs.

WSN are common to experience different attacks because of their broadcast medium of data transfer. Attacks are commonly divided in active and passive attacks. Passive attacks are those that do not harm system in its core, however unwanted party is able to see transported data. Monitoring, eavesdropping, traffic analysis and camouflage adversaries are the most common attacks on WSN's privacy, which is snooping and discovering hidden data by attackers. Active attacks are those that that modify transferred data, and they come in numbers. Routing attacks spoofed and altered routing information. Selective forwarding or dropping certain packets from transport. Sinkhole attack or redirecting all traffic to specific node. Sybil attack, single node is cloned has multiple identities. Wormholes attack, tunneling packets to different locations. Denial of Service (DoS), attack in which multiple request are sent to a victim overloading it and disabling legit users to use the service. Node malfunction, node generates inaccurate data. Physical attack previously discussed belongs to group of active attacks. False node which generates false data and message corruption [10].

Remote sensor organizing keeps on developing as a standout amongst the most energizing and testing research regions within recent memory. Characteristically, there are numerous utilizations of remote sensor organizes that gather and disperse touchy and critical data. All together for some usage of these applications to work effectively, it is important to keep up the protection and security of the transmitted information. What stays indistinct, in any case, is a pleasing and best method for anchoring the data. This paper considers mainstream and dynamic security models accessible and used to-date, while concentrating on verification. Confirmation can be characterized as a security system, the utilization of which permits the personality of a hub in the system to be distinguished as a legitimate hub of the system. Information realness can be accomplished when a legitimate hub unscrambles the affixed message verification code, or applies one to an active bundle, utilizing some known/shared key. Hub confirmation can be accomplished utilizing various distinctive techniques. A correlation table is exhibited which shows the different properties held by these security conventions, counting verification attributes. This will permit the alluring qualities of the different security models to be effortlessly recognizable to originators in their battle to execute the most practical and suitable strategy for anchoring their system [11].

CareNet is an incorporated remote sensor condition for re-bit social insurance that utilizes a two-level remote system and an extensible programming stage. CareNet gives both profoundly dependable and security mindful patient information accumulation, transmission and access[12]. This paper portrays our framework architecture, programming advancement, and the aftereffects of our field studies [13].

To the best of our insight no dispersed arrangement has been proposed to distinguish a hub catch in a versatile remote sensor network[14]. In this paper we propose a productive and circulated answer for this issue utilizing new properties of portable remote sensor systems. Specifically, we present two arrangements: SDD that does not require express information trade between the hubs amid the nearby discovery, and CCD, an increasingly advanced convention that utilizes neighborhood hub collaboration notwithstanding versatility to enormously enhance performance. We likewise acquaint a benchmark with contrast these arrangements and. Trial results show the feasibility of our proposition. For example, while the benchmark requires around 9,000 seconds to distinguish hub catches, CDD requires under 2,000 seconds. These outcomes bolster our instinct that hub versatility, related to a constrained measure of nearby participation, can be utilized to identify rising worldwide properties [15].

A focal issue in sensor arrange security is that sensors are vulnerable to physical catch assaults. When a sensor is endangered, the enemy can undoubtedly dispatch clone assaults by duplicating the bargained hub, conveying the clones all through the system, and beginning an assortment of insider assaults. Past neutralizes clone assaults experience the ill effects of either a high correspondence/stockpiling overhead or a poor recognition precision. In this paper, we propose a novel plan for identifying clone assaults in sensor networks, which processes for every sensor a social unique finger impression by removing the area attributes and confirms the authenticity of the originator for each message with a money ordering the encased unique finger impression. The unique mark age depends on the superimposed s-disjunct code, which causes a light correspondence and calculation overhead. The unique mark check is led at both the base station and the neighboring sensors, which guarantees a high detection likelihood. The security and execution investigation demonstrate that our calculation can distinguish clone assaults with a high identification likelihood at the expense of a low computation/correspondence/stockpiling overhead. To our best knowledge, our plan is the first to give real-time identification of clone assaults in a compelling and effective way [16].

Remote Sensor Networks (WSNs) are another innovation foreseen to be utilized progressively sooner rather than later because of their information securing and information preparing capacities. Security for WSNs is a territory that should be considered so as to ensure the usefulness of these systems, the information they pass on and the area of their individuals. The security models and conventions utilized in wired and different systems are not suited to WSNs due to their extreme asset imperatives, particularly concerning vitality. In this article, we propose a brought together interruption recognition conspire dependent on Support Vector Machines (SVMs) and sliding windows. We find that our framework can recognize dark opening assaults and particular sending assaults with high exactness without exhausting the hubs of their vitality [17][18].

Data conglomeration in remote sensor systems is essential because of its upgrade of transmission capacity use and vitality usage by limiting the exchange of excess information[19]. This paper displays a safe information accumulation convention, called SRDA, for remote sensor systems. So as to decrease the quantity of bits transmitted, SRDA requires sensor hubs to send differential information rather than crude detected information. Viability of the SRDA is additionally exhibited by applying its key component to improve existing information collection conventions. SRDA sets up secure network among sensor hubs by exploiting organization estimation and not playing out any online key appropriation. The gradual security prerequisite because of the idea of the information conglomeration process is met by a total explicit security strategy. Recreation results demonstrate that SRDA yields huge investment funds in the vitality utilization while protecting the information security [20].

In this paper, authors proposed another down to earth personality based encryption plot which is reasonable for remote sensor network (WSN). We call it Receiver-Bounded Online/Offline Identity-based Encryption (RB-OOIBE). It parts the encryption process into two sections – the disconnected and the on-line part. In the disconnected part, all overwhelming calculations are managed without the information of the collector's character and the plaintext message. In the online stage, just light computations, for example, secluded activity and symmetric key encryption are required, together with the collector's character and the plaintext message. In addition, since each disconnected ciphertext can be re-utilized for a similar recipient, the quantity of disconnected ciphertexts the encrypter holds just limits the quantity of collectors rather than the quantity of messages to be scrambled. Along these lines, a sensor hub (with constrained computation power and restricted stockpiling) in WSN can send encoded information effortlessly: A couple disconnected ciphertexts can be figured in the assembling stage while the online part is light enough for the sensor to process[21][22].

The insurance of basic frameworks ace vides a fascinating application region for remote sensor systems. Dangers, for example, common catastrophes, and criminal or psychological oppressor assaults against CIs are progressively announced. The substantial scale nature of CIs requires an adaptable and minimal effort technology for enhancing CI checking and reconnaissance. WSNs are a promising possibility to satisfy these prerequisites, yet on the off chance that the WSN turns out to be a piece of the CI so as to enhance its unwavering quality, at that point the constancy of the WSN itself should be altogether enhanced first. In this article we discuss the difficulties and potential answers for accomplish steadfastness of WSNs considering coincidental disappointments and purposeful assaults. We investigate the entire framework beginning from individual sensor hubs through the convention stack to the middleware layer above. With the across the board development of utilizations of Wireless Sensor Networks (WSNs), the requirement for dependable security instruments these systems have expanded complex. Numerous security arrangements have been proposed in the area of WSN up until now. These arrangements are normally dependent on surely understood cryptographic calculations. In this paper, we have tried to overview surely understood security issues in WSNs and concentrate the conduct of WSN hubs that perform open key cryptographic tasks. We assess time and power utilization of open key cryptography calculation for signature and key administration by reproduction [23].

WSNs typically conveyed in the focused-on region to screen or detect nature and relying on the application sensor hub transmit the information to the base station. To relay the information middle hubs, impart together, select proper steering way and transmit information towards the base station. Directing way determination relies upon the steering master tool of the system. Base station ought to get unaltered and new information. To satisfy this prerequisite, steering convention ought to be vitality proficient and secure. Various leveled or group base steering convention for WSNs is the most vitality productive among other directing conventions. In this paper, we ponder different various leveled directing method for WSNs. Further we break down and look at secure progressive steering conventions dependent on different criteria [24].

The utilization of remote sensor organize (WSN) for a water quality checking is made out of various sensor hubs with a systems administration capacity that can be sent for an impromptu or ceaseless observing reason. The parameters associated with the water quality assurance such as the pH level, turbidity and temperature is estimated in the constant by the sensors that send the information to the base station or control/checking room. This paper proposes how such observing framework can be setup underlining on the parts of minimal effort, simple impromptu establishment and simple dealing with and upkeep. The utilization of remote framework for checking reason won't just diminish the general observing framework cost in term of offices setup and work cost yet will likewise give adaptability in term of separation or area. In this paper, the essential plan and usage of WSN including a powerful transmission Zigbee based innovation together with the IEEE 802.15.4 good handset is proposed. The created stage is practical and permits simple customization. A few fundamental consequences of estimation to assess the dependability and adequacy of the framework are additionally exhibited[25][26].

CitySense is a new idea of coverage whole cities with wireless sensor in order to make networking testbed for the further research. For the implementation are used 100 Linux based PCs and 802.11a/b/g radios and other sensors. Benefit of this kind of services is that sensors nodes can be changed and programmed by end users. Security issues is big deal when it comes to public environment so CitySense use two-layer approach to security, WPA encryption at link layer to prevent unwanted listeners and Secure Socket Layer or Secure Shell in transport layer to secure safe communication. WPA keys are periodically changed using STP because of possibility of cracking it[27][28].

BROSK (Broadcast session Key) negotiation protocol is new proposition of secure protocol that will perform better than existing ones SPINS and SNAKE. These two well-known protocols could outperform BROSK when it comes to number of nodes less than 64, but BROSK is designed for systems with greater number of nodes and of course less energy needed to perform. Our main concern is security and this protocol is best at it because it broadcasts once for each node and if it receives some additional request it will know that malicious node is approaching so it will mark that node as malicious one and will not make troubles any more [29].

For the greatest challenge in network security, implementation of cryptographic primitives, there is one nice proposition to solve it, NOVSF (nonblocking orthogonal variable spreading factor) code hopping technique, which have 64-time spots that could be given to any channel. This is used to periodically change the way of how data will be assigned to these time slots and because of this some unwanted users will firstly have to crack this pattern of assigning data to time slots and then do decrypting of data. This is possible because one multiplexer is added to system, and no additional energy is needed to accomplish this higher level of security [30].

Widely use of wireless sensor network is becoming real in our era and with it comes responsibility of preserving accurate data and saving it from malicious users. There are many ways to accomplish that goal. Data secrecy is accomplished throughout some standard encryption methods such as AES block cipher as sharing secret key between the communication partitions. But encryption is not enough because data is still vulnerable for attacks such as eavesdropping. To prevent this kind of behavior, encryption have to be enforced with access control policy at its base station[31][32].

WSN can play important role in preservation of our environment by monitoring observations in nature, as it found its purpose in Forest-Fires Surveillance System (FFSS). Sensors collect data about climate changes in dry winter season. Information are collected and people can check conditions in mountains, even it can trigger alarm if there is smoke or fire to prevent bigger disasters[33]. When it comes to security of collected date, we can see that Minimum Cost path Forwarding protocol is used, optimal, simple and scalable way of transferring the data where nodes can be found limited number of times in one round in order not to suck energy form upstream nodes [34].

Sleep Deprivation Attack is most dangerous attack of this category in which intruders cause random drainage of sensor node batteries to dramatically shorten its lifetime. By detecting the SPA lifetime of a sensor nodes batteries and the network itself will be prolonged. Anomaly detection is used to compare values with predefined parameters to see if there is any intruders who are trying to harm the network and when found those malicious nodes are excluded [35].

For the prevention of the denial of service (DoS) we will introduce one interesting protocol. We should mention that we have two types of the DoS attacks, nodes which uses network for its own purposes and communication (passive attacks) and harming other nodes unintentionally, and malicious nodes that intentionally want to harm other nodes by not using energy efficiently (active attacks). As it is in wireless sensor network, nodes need to forward messages to other nodes but in some cases, they cannot do that. This protocol acts as a game theory to recognize those nodes that could act maliciously [36].

Besides the environmental benefits which we saw in FFSS, WSN found its application in many other fields with such as emergencies, military, health monitoring etc. And that's why security is fundamental requirement of these sensor applications. In this case we will focus on physical threats for these services. Physical attacks can put whole sensor network to operate on its minimum because of limited physical access. Some of the issues in WSN are: Availability, Secure localization, Self-organization, Authenticity, Flexibility and others [37].

Data aggregation is one of the important concepts in wireless sensor network due to energy consumption and saving resources. Aim of this concept is to eliminate redundant data conveyance. This data aggregation can be done by one sensor or more of them combined and collecting data from other sensors. Data aggregation approaches in WSN are: tree base approach, cluster-based approach, multi path approach and hybrid approach. The main concern in data aggregation security are data integrity and data confidentiality [38].

WSN are also used in monitoring services[39]. Main concern of security in this usage of wireless sensor network is privacy preserving location. To achieve this goal of anonymity two algorithms are used, resource and quality aware. Resource algorithm is used for keeping data about location private and reduces the cost of communication between sensors and required computations. Quality aware algorithm minimizes the size of search area in order to get more accurate location [40].

3. CONCLUSION

In contrast to different systems, WSNs are intended for explicit applications. Applications incorporate, however are not constrained to, ecological observing, mechanical machine checking, reconnaissance frameworks, and military target following. Every application contrasts in highlights and requirements. To help this decent variety of utilizations, the development of new correspondence conventions, calculations, structures, and administrations are required. We have overviewed in this paper issues on three unique classes: (1) inside stage and basic working framework, (2) correspondence convention stack, and (3) organize administrations, provisioning, and sending issues. We have condensed and looked at changed proposed structures, calculations, conventions, and administrations. In addition, we have featured conceivable enhancements and research in each territory. There are as yet numerous issues to be settled around WSN applications, for example, correspondence structures, security, and the executives. By settling these issues, we can close the hole among innovation and application.

REFERENCES

[1] Y. Liu, “Wireless sensor network applications in smart grid: Recent trends and challenges,” *Int. J. Distrib. Sens. Networks*, vol. 2012, 2012.

[2] H.-R. Tseng, R.-H. Jan, and W. Yang, “An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks,” *IEEE GLOBECOM 2007-2007 IEEE Glob. Telecommun. Conf.*, pp. 986–990, 2007.

[3] T. Naeem, “Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks,” *Int. J. Digit. Content Technol. its Appl.*, vol. 3, no. 1, pp. 88–93, 2009.

[4] R. Nave, “Crossed Polarizers,” 2012.

[5] R. Sharma, Y. Chaba, and Y. Singh, “Analysis of Security Protocols in Wireless Sensor Network,” *Int. J. Adv. …*, vol. 713, pp. 707–713, 2010.

[6] J. S. Lee, Y. W. Su, and C. C. Shen, “A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi,” *IECON Proc. (Industrial Electron. Conf.*, pp. 46–51, 2007.

[7] S. R. Jino Ramson and D. Jackuline Moni, “Applications of Wireless Sensor Networks - A survey,” *Proc. IEEE Int. Conf. Innov. Electr. Electron. Instrum. Media Technol. ICIEEIMT 2017*, vol. 2017–Janua, no. July, pp. 325–329, 2017.

[8] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, “Decentralized intrusion detection in wireless sensor networks,” *Proc. 1st ACM Int. Work. Qual. Serv. Secur. Wirel. Mob. networks - Q2SWinet ’05*, p. 16, 2005.

[9] R. Roman, J. Zhou, and J. Lopez, “Applying Intrusion Detection Systems to Wireless Sensor Networks,” no. Ccnc, pp. 640–644, 2006.

[10] D. G. Padmavathi and M. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 1 & 2, p. 9, 2009.

[11] D. Boyle and T. Newe, “Security protocols for use with wireless sensor networks a survey of security architectures,” *Third Int. Conf. Wirel. Mob. Commun. 2007, ICWMC ’07*, no. May, 2007.

[12] P. Li, C. Xu, Y. Luo, Y. Cao, J. Mathew, and Y. Ma, “CareNet: Building Regulation-Compliant Home-Based Healthcare Services with Software-Defined Infrastructure,” *Proc. - 2017 IEEE 2nd Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol. CHASE 2017*, pp. 373–382, 2017.

[13] S. Jiang *et al.*, “CareNet: An Integrated Wireless Sensor Networking Environment for Remote Healthcare,” *Proc. 3rd Int. ICST Conf. Body Area Networks*, no. May 2014, 2008.

[14] Y. K. Kim, K. S. Kim, and S. Kim, “A portable and remote 6-DOF pose sensor system with a long measurement range based on 1-D laser sensors,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 9, pp. 5722–5729, 2015.

[15] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, “Emergent properties: detection of the node-capture attack in mobile wireless sensor networks,” *Proc. first ACM Conf. Wirel. Netw. Secur.*, pp. 214–219, 2008.

[16] K. Xing, X. Cheng, F. Liu, and D. H. C. Du, “Real-time detection of clone attacks in wireless sensor networks,” *Proc. - 28th Int. Conf. Distrib. Comput. Syst. ICDCS 2008*, pp. 3–10, 2008.

[17] S. Kaplantzis, A. Shilton, N. Mani, and A. Sekercioglu, “Detecting Selective Forwarding Attacks in WSN Using Support Vector Machines,” *Issnip*, pp. 335–341, 2007.

[18] M. V. Ramesh, A. B. Raj, and T. Hemalatha, “Wireless sensor network security: Real-time detection and prevention of attacks,” *Proc. - 4th Int. Conf. Comput. Intell. Commun. Networks, CICN 2012*, pp. 783–787, 2012.

[19] G. D. O’Mahony, P. J. Harris, and C. C. Murphy, “Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018–October, pp. 1–5, 2018.

[20] H. O. Sanli, S. Ozdemir, and H. Cam, “SRDA: secure reference-based data aggregation protocol for wireless sensor networks,” *IEEE 60th Veh. Technol. Conf. 2004. VTC2004-Fall. 2004*, vol. 7, no. C, pp. 4650–4654, 2004.

[21] D. W. Li, G. Yang, H. Y. Su, and Y. L. Chen, “An ID-based broadcast encryption scheme for hierarchical wireless sensor networks,” *2nd Int. Conf. Inf. Sci. Eng. ICISE2010 - Proc.*, vol. 2, pp. 1834–1837, 2010.

[22] C.-K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, “Practical ID-based encryption for wireless sensor network,” *Proc. 5th ACM Symp. Information, Comput. Commun. Secur. - ASIACCS ’10*, no. January, p. 337, 2010.

[23] L. Buttyán, D. Gessner, A. Hessler, and P. Langendoerfer, “Application of wireless sensor networks in critical infrastructure protection: Challenges and design options,” *IEEE Wirel. Commun.*, vol. 17, no. 5, pp. 44–49, 2010.

[24] S. Sharma and S. K. Jena, “A survey on secure hierarchical routing protocols in wireless sensor networks,” *Proc. 2011 Int. Conf. Commun. Comput. Secur. - ICCCS ’11*, p. 146, 2011.

[25] S. N. Rana and P. Kamboj, “Resource utilization based congestion control for wireless sensor network: A review,” *Proc. 10th INDIACom; 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2016*, pp. 715–720, 2016.

[26] S. Sridharan, “Water Quality Monitoring System Using Wireless Sensor Network,” *Int. J. Adv. Res.*

Electron. Commun. Eng., vol. 3, no. 4, pp. 399–402, 2014.

[27] A. Salmins, K. Ozols, and R. Ruskuls, “Data management in TestBed for large scale wireless sensor networks,” *Proc. - 2015 Adv. Wirel. Opt. Commun. RTUWO 2015*, pp. 54–57, 2015.

[28] R. N. Murty *et al.*, “CitySense: An urban-scale wireless sensor network and testbed,” *2008 IEEE Int. Conf. Technol. Homel. Secur. HST’08*, no. December, pp. 583–588, 2008.

[29] B. Lai, S. Kim, and I. Verbauwhede, “Scalable session key construction protocol for wireless sensor networks,” *IEEE Work. Large Scale Realt. Embed. Syst.*, 2002.

[30] H. Çam, S. Özdemir, D. Muthuavinashiappan, and P. Nair, “1章 小児期・思春期の成長・発達・心のとらえ方. Pdf,” pp. 2981–2984, 2003.

[31] Y. Jin, X. Guo, R. G. Dutta, M. M. Bidmeshki, and Y. Makris, “Data Secrecy Protection Through Information Flow Tracking in Proof-Carrying Hardware IP - Part I: Framework Fundamentals,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 10, pp. 2416–2429, 2017.

[32] E. Shi and A. Perrig, “Designing secure sensor networks,” *IEEE Wirel. Commun.*, vol. 11, no. 6, pp. 38–43, 2004.

[33] L. Shkurti, X. Bajrami, E. Canhasi, B. Limani, S. Krrabaj, and A. Hulaj, “Development of ambient environmental monitoring system through wireless sensor network (WSN) using NodeMCU and ‘WSN monitoring,’” *2017 6th Mediterr. Conf. Embed. Comput. MECO 2017 - Incl. ECYPS 2017, Proc.*, no. June, pp. 1–5, 2017.

[34] B. Son, Y. Her, and J. Kim, “A design and implementation of forest-fires surveillance system based on wireless sensor networks for South Korea mountains,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 9, pp. 124–130, 2006.

[35] T. Bhattasali, R. Chaki, and S. Sanyal, “Sleep Deprivation Attack Detection in Wireless Sensor Network,” *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19–25, 2012.

[36] A. Agah and S. K. Das, “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach,” *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 145–153, 2007.

[37] R. W. Anwar, M. Bakhtiari, A. Zainal, A. Hanan Abdullah, and K. N. Qureshi, “Security issues and attacks in wireless sensor network,” *World Appl. Sci. J.*, vol. 30, no. 10, pp. 1224–1227, 2014.

[38] K. Maraiya, K. Kant, and N. Gupta, “Wireless Sensor Network: A Review on Data Aggregation,” *Ijser.Org*, vol. 2, no. 4, pp. 1–6, 2011.

[39] S. Padwal, A. Holkar, S. Khote, P. Maral, and V. Kadam, “Using wide area monitoring WSN,” *2017 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2017*, no. Icices, 2017.

[40] K. P. Kaliyamurthie, D. Parameswari, and R. Udayakumar, “QOS aware privacy preserving location monitoring in wireless sensor network,” *Indian J. Sci. Technol.*, vol. 6, no. SUPPL5, pp. 4648–4652, 2013.