Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 14, March 2018 – www.caeaccess.org

Evolution of Cryptographic Algorithm for Resource Constrained Wireless Networks: An Investigation Approach

Tejashwini N.
Research Scholar
Visvesvaraya Technological University, Belagavi, Karnataka, India

D. R. Shashi Kumar, PhD
Head of Department CSE,
Cambridge Institute of Technology, Bengaluru, Karnataka, India

K. Satyanarayana Reddy, PhD
Head of Department ISE
Cambridge Institute of Technology, Bengaluru, Karnataka, India

ABSTRACT
In the era of the internet of things, provisioning suitable security models for small and resource constrained nodes as well in-network requires consideration of synchronization among heterogeneous operating conditions. This paper provides an investigational study of traditional approaches adopted for resource constrained wireless networks especially Wireless Sensor Network (WSN). The inferring of basic assumptions to propose customized algorithms is discussed to provide an insight into the development of suitable cryptographic and security approaches for future generation WSN that will be a sub-system of Internet-of-Things (IoT). The methodology adopted for investigation includes consideration of recent state of art work published in archival journals including IEEE, Springer, Elsevier, and special edition journals. Initially, approximately 400 plus journals are referred and later articles from various sources since 2015 is considered for an intrinsic explanation of algorithmic consideration, its pros, and cons with a citation to show the potential of its evolution. The outcomes of the paper as statistics, concept, and classification are useful for security specialist researchers and academicians.

Keywords
Wireless Network, Internet-of-Things, Cryptography, Security Algorithm

1. INTRODUCTION
The study of Wireless Sensor Network (WSN) was an independent study from past two decades. Initially, the focus of the study was on issues related to hardware architecture to provide miniaturization of all the sub-units including sensory, microcontroller and radio [1], as initially the use of WSN were limited to organizations of critical mass such as defense, space, and other critical domains of applications. Therefore, customization of the hardware, software, and firmware to suit the targeted application of this domain were the prime focus of this research. With the evolving advancement and cost reduction in the constituent of the WSN including 1) cost of sensors 2) sensor nodes 3) bandwidth as well as 4) communication protocols, the application of WSN has moved to various fields such as 1) structural health monitoring (SHM), 2) intrusion detection system (IDS), 3) critical climate change monitoring system (CCCM), 4) environmental monitoring, 5) habitat monitoring and many more pervasive and ubiquitous based applications in the field of healthcare, industry, monitoring of micro-grid station and today smart applications using WSN as sub-system of IoT [2-9]. These applications are quite useful for the population exploring the world to meet the vision of industry 4.0 [10], but at the same time, the scalability and the popularity of WSN make it vulnerable, poses its kind of security threats, risk, and challenges. This paper thoroughly investigates these vulnerability, attacks, solutions, and pathway to the future research to meet the optimal goal of security dimension to the WSN to ensure a true sense real-time adaptable network for the human society in the different walk of life. Section II describes the research methodology to survey the security requirements and attacks in the context of WSN. Section III describes security requirements and attacks in WSN, whereas section IV explicitly explains cryptography and key management challenges in WSN. Finally, section V concludes the paper.

2. INVESTIGATIONAL STUDY METHODOLOGY
To find relevant work in the field of WSN an IEEE and Inspect keyword 'Wireless Sensor Networks' is considered which shows the first timestamp of the publication from 1907. The typical classification of articles since 1907 till 6th February 2018 is shown in Table 1.

Table 1: Statistics of Publication Indexed in IEEE Xplore for keyword "Wireless Sensor Network"

Conference	Journals & Articles	Early Access Articles
59,774	9,315	358

Further classification purpose of various problems of research in the domain of WSN only journals of last 5 years, i.e., 2013 till 2018 February is taken in consideration and Fig.1 and Fig.2 shows the statistics of overall research and classification respectively. The number of journals found is 4, 936.

Table 2: Statistics of Journal Publication since 2013 till February 2018

Year	2013	2014	2015	2016	2017	2018(till 6th Feb)
No.	759	865	1,001	1,096	1,099	116

The statistics reveal that there is an increasing potential in the research of WSN issues and yet it is an open and very active research problem. Further, the trend of research from the viewpoint of security is analyzed with a sub-search keyword of security and Table 3 illustrates the statistics of the research trend in a security problem domain since 2013 till 6th February 2018.

Table 3: Statistics of Journal Publication since 2013 till February 2018 for Security problem domain

Year	2013	2014	2015	2016	2017	2018(till 6th Feb)
No.	77	95	98	116	140	11

Table 3 also exhibits the increasing trend of research in the security domain in the wireless sensor network. Table 4 illustrates percentage stake of security research in overall.

Table 4: Percentage of Security Problem Research Statistics Since 2013

Year	2013	2014	2015	2016	2017	2018(till 6th Feb)
Overall	759	865	1,001	1,096	1,099	116
Security	77	95	98	116	140	11
% of Security research	10.14	10.98	5.59	10.58	12.73	9.48

The average stake of only security research is found approximately 9.916% say 10%, which shows the importance and activeness of study requirement.

3. SECURITY REQUIREMENT AND ATTACKS

In this section, firstly the different security requirements in the context of WSN is described in sub-section 3.1 followed by various attacks in WSN in Section 3.2.

3.1 Security Requirements in WSN

There are different dimensions to look into internal and external security requirements in the context of WSN. One of the approaches could be to analyze different operations of WSN stack synchronous to different layers of the network. The operations of data aggregation take place at application layer, where the security threats could be to bring deficiency to the content of the data and affects overall reliability whereas a transport layer the responsibility of timely delivery can be modified by means of injecting some mechanism which introduces delay and affects the reliability of data delivery to extent the end to end delay. Many attacks can be performed at the network layer where the typical route-finding process is performed, and attacks can mislead the falsified routes. There are many operations takes place at the physical layer to handle the radio frequency propagation from one node to another node, which includes mechanism of frequency and channel selection, various signal processing, operations, and modulations. Creating any modifications may lead the complete network failure using error maximization of the frames or biased scheduling of radios and exhausting energy to make the network dead [11]. The typical distinguishing characteristics which make WSN vulnerable against security threats includes: 1) Self-organization: The random deployment and reconfiguration of network topology in situation of node failures is achieved by self-organizing capacity by adopting adhoc technology, which makes WSN flexible to get implanted attackers node seamlessly [12]., 2) Self-adaptive flow control: The adverse transmission controls is achieved against erroneous transmission based on link quality [13], 3) Resource Restriction: Only the usage of lightweight solutions towards enhancing security features within a node is supported at present where such approaches are resistive towards external intrusion, but it doesn't offer extensive resiliency against internal attacks [14]., 4) Centralized Control: Although sensor nodes work on centralized architecture, the existing routing mechanism are so diversified that they don't offer robust security consideration [15], 5) Open environment: In contrast to the earlier days where WSN were deployed only in the human inaccessible area, today it is deployed to the human accessible area so intruder can easily do physical man handling of the nodes as a node capture. The captured node is helpful to know the internal architecture understanding of the difference processes and protocols and initiates different attacks [16].

The traditional approach towards security provisioning in WSN considers three basic requirements 1) confidentiality: Which is achieved by means of cryptography at physical layer to encrypt node data transmission in order to protect the confidentiality [17], 2) Integrity: the automatic message code update influences the integrity of the data [18], 3) Availability: The uptime of the WSN depends upon the remaining energy which can be influenced by engaging the network by means of false crowd or flood kind of effects [19]. Apart from these traditional considerations, WSN needs to consider many another critical requirement which is sensitive to the data exchange mechanism when integrated into the complex systems like pervasive, ubiquitous, and IoTs [20].

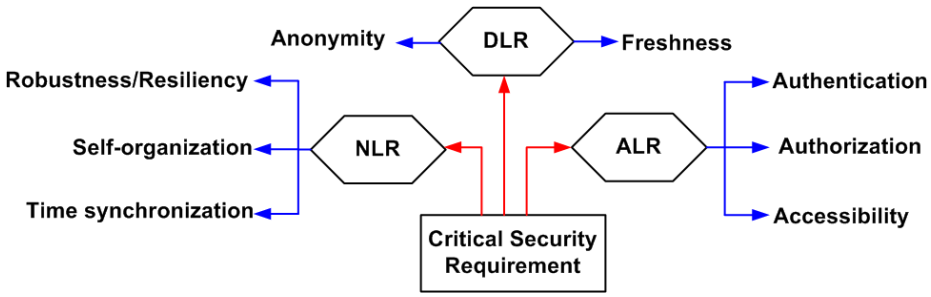

Fig 1: Critical Additional Security Requirements of WSN

The efficient design consideration of security framework also depends upon the specification of devices/nodes, the kind of technologies adopted for network and specific application requirements along with above discussed general and critical specification.

A. Attacks in WSN: The different attacks perform at the different layers is shown in Figure 2, where layer-wise attacks with its type either external or internal is described

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 14, March 2018 – www.caeaccess.org

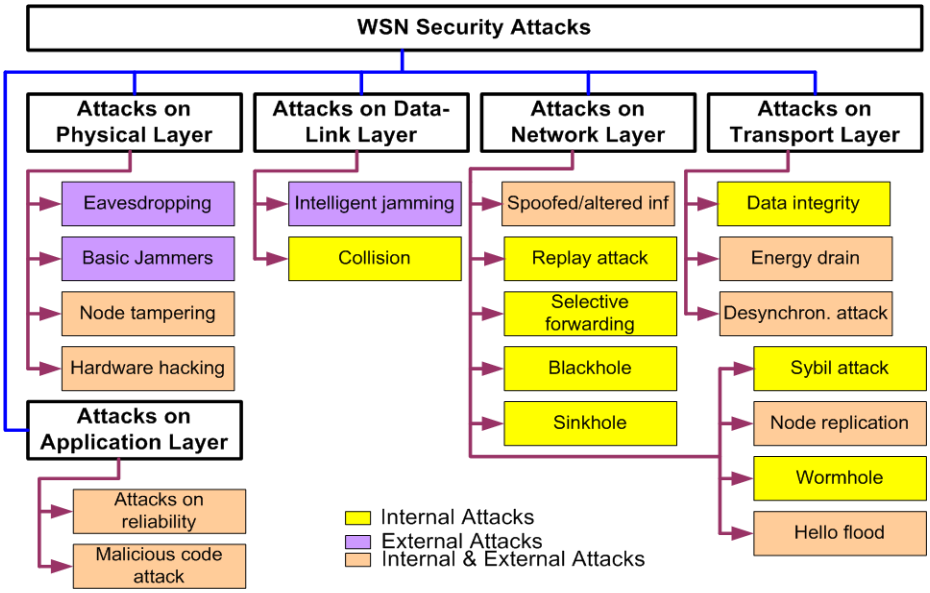

Fig 1: Taxonomies of WSN Security Attacks [20]

Figure 2 exhibits the different forms of the critical attacks that has been investigated by the researcher towards enhancing the security feature of the WSN. The briefing of the attacks is carried out considering different layers of the protocol stack of WSN as follows:

- ***Physical Layer Attacks*:** Such forms of attacks mainly target the signal transmission process that finally leads the sensor node to become prone to malicious codes resulting in fully or partially capturing of the controls of the node. The critical forms of attacks in these layers are eavesdropping, jamming, node tampering, and hardware hacking. They can be both external and internal forms of attack. Eavesdropping leads to intercepting the ongoing signal transmission while jamming leads to disruption of the transmission. Node tampering results in complete or partial tampering of the sensor while hardware hacking results in physical damage to the sensor. At present times, there have been various attempts to evolve up with solution towards securing against such attacks. Table 5 highlights some of the research approaches that are conventionally used in an existing system for resisting physical layer security.

Table 5: Existing Research towards addressing Physical Layer Attacks

Authors	Attacks	Methods	Performance Metric	Outcome
Wu et al. [21]	Eavesdropping	Gossip algorithm, non-negative matrix theory	variance	Faster convergence
Proano et al.[22]	Eavesdropping	Decorrelation of traffic	Delay	Reduce overhead by 50%
Tiloca et al. [23]	Basic Jammers	Decentralized TDMA scheme	Energy, join probability	Reduces overhead
Heo et al. [24]	Basic Jammers	Multi-channel hopping	Packet delivery performance	Increased packet reception ratio by 98%
Bodkhe & Raut [25]	Basic Jammers	Usage of trigger nodes	Energy	Energy efficient
Nunoo-mensah [26]	Node Tampering	Hashing, packet-based authentication	Energy, Processing time	Energy efficient
Salmasi [27]	Node Tampering	Interactive-based method, hardware-based	Rotor speed,	Fault-tolerant
Duan [28]	Node Tampering	Ring model for tamper resistance, 3DES, HMAC	Recovery time	Offer improved stability

- ***Data Link Layer Attacks*:** The attack on data link layer is majorly focused on controlling the traffic flow from a specific target node. Such forms of attacks occur owing to the vulnerable usage of the shared medium when attempted access by various concurrent sensors. Transmission errors are also caused owing to the data link layer attacks. It has also been found that majority of the attacks are closely associated with the MAC layer in data link layer. Two potential attacks in this layer are intelligent jamming attack and collision attack. The former kind of attack leads to disclosure of data distribution channels while the latter form of attack leads to the potential form of the collusion among the sensors. The existing approaches towards mitigating such forms of attacks are as tabulated below in Table 6.

Table 6: Existing Research towards addressing Data Link Layer Attacks

Authors	Attacks	Methods	Performance parameters	Outcome
Babar et al. [29]	Intelligent Jamming	Clustering	Delay, energy, throughput	Increase resiliency by 20%
Dbibh et al. [30]	Collision	Collision-avoidance MAC scheme	Latency, energy, throughput	Improve communication
Ismail et al. [31]	Collision	Improved error correction, decoding, hardware-based	Correlation, bit error rate, throughput, energy	Reduced latency

- ***Network Layer Attacks*:** This layer always acquires the complete attention of attackers as this layer is responsible for managing routing protocols. This layer offers communication channel to perform data forwarding operation in WSN. There are large ranges of attacks in this layer, and large numbers of researchers have already offered a different form of solution to resist such forms of attacks. However, an attack on this layer is yet to find its effective solution. Some of the significant approaches towards solving security issues arising from network layer-based attacks are as follows:

Table 7: Existing Research towards addressing Network Layer Attacks

Authors	Attacks	Methods	Performance parameters	Outcome
Almomani et al. [32]	Blackhole attack	Machine learning	accuracy	Better accuracy in attack identification
Qin et al. [33]	Replay attack	Key management, HMAC	Packet delivery ratio, energy,	Good communication
Zhang et al.[34]	Selective forwarding	Network coding	Decoding rate, energy, time	Resistive against flooding attack
Han et al.[35]	Sinkhole	Neighboring node, ad-hoc routing,	Accuracy, energy, packet loss	Energy efficient
Dong and Liu [36]	Sybil attack	Time synchronization, graph theory	Difference in messages	Resistive against jamming and DoS attack too
Zhou and Wang [37]	Node replication	Identification of attacks, digital signature	Detection probability	Minimize overheads
Singh et al. [38]	Wormhole	Delphi Scheme, Watchdog, probability	Accuracy, Correlation	Computationally cost-effective
Karapistoli [39]	Hello flood	The ultra-wide band, anomaly detection	Detection accuracy	Energy efficient

- ***Transport Layer Attacks*:** In this layer, one kind of attack takes place where the integrity of the data is compromised in the process of the transmission where the false message is injected. This process severely affects the routing aspect. At the same time, a kind of attack also takes place where an enormous amount of the connectivity is established, which in turns exhaust the resource of the nodes and as a result entire energy is drained. One another type of attack namely desynchronizes where the forged kind of message brings a request session to affect the synchronization is lost due to which there exist broken communication link and transmission routes are compromised and affects overall performance.

Table 8: Existing Research towards addressing Transport Layer Attacks

Authors	Attacks	Methods	Performance Parameters	Outcome
Yan et al. [40]	Data integrity	Theoretical and Statistical	Variation percentage of δ is an absolute value	Accurate detection of data integrity attack
Nam et al. [41]	Energy Drain	Genetic algorithm	Energy	Improvement in energy against the drain
Song et al. [42]	delay attack	Generalized extreme studentized deviate (GESD) algorithm and time transformation technique	Success rate, accuracy improvement rate, synchronize interval rate, delay attack time	Effective against delay attack, successful detection rate, false positive rate, and accuracy improving rate.

- ***Application layer:*** In these kinds of attack which takes place on application layer is of both external and internal type which is initiated by generating wrong or false kinds of queries. These attacks are known as an attack on the reliability. Another attack in application layer where the injected warm compel to lose the proper functioning of services that happens because of energy harassment and Collison. And finally, the overall network degrades.

Table 9: Existing Research towards addressing Application Layer Attacks

Authors	Attacks	Methods	Performance parameters	Outcome
Geethu and Mohammed al. [43]	Selective forwarding attack	Defense mechanism	Reliability, Data delivery ratio	Improvement in the efficiency of network and QoS parameter
Diaz et al. [44]	Wormhole attack	Statistical	Dropped packet ratio	Minimalization of packet draw

4. CRYPTOGRAPHY AND KEY MANAGEMENT CHALLENGES IN WSN

The WSN operates on low power electronics with very limited storage and memory buffer in the microcontroller unit of the sensor node. Apart from another processing, the modulation takes the higher amount of power consumption. Therefore, the cryptographic algorithm and key management process require customized provisioning to meet the balance between additional overhead between security that should be compensated in another operation of routing. The significant work towards synchronized cryptographic algorithm along with customized key management is witnessed since 2004. Approximately 82 journals have been found where the cryptographic process for the security in WSN is used.

Xiangqian et al. (2009) have conducted a survey related to the security aspect in WSN. In their observation, the entire issues of the security are classified into seven distinguished categories as shown in fig 3 [45].

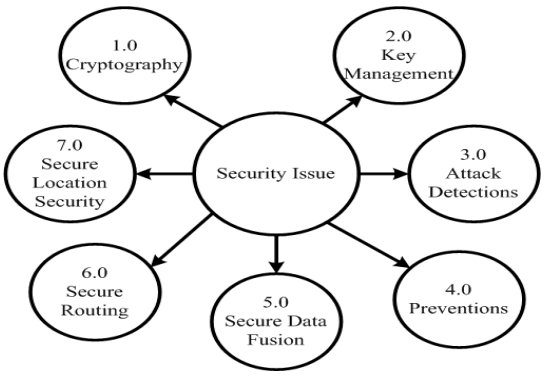

Fig2: Classification of Security Aspects

Cryptography approach is having its challenges from the view point of computational resource requirements along with effective key management as per the typical context. The cryptography method must meet the typical constrains of sensor nodes and the network. RC-4/RC-5 performance better as compared to other symmetric encryption and has a function such as SHA1, MD5, and IDEA when evaluated in the work of **Ganesh et al. (2003)** [46], **Perrig et al. (200**2), [47].

A typical WSN namely body sensor network (BSN) need critical security solution as it gathers very personal information which relies on the identity as well as on the mechanism of key distribution. Therefore the traditional method adopted for the general WSNs does not fit well. In the work of **Huang et al. (2013),** use of a Diffie-Hellman version of elliptic curve hashing is exploited for dynamic key distribution to overcome the adverse effects of pre-key distributions [48]. The approach of identity-based approach is used for node authentication to handle the challenges and problems faces for key agreement. These methods do not use computationally over headed certificates that make it suitable for the wins as well reduces the consumption of the resources for operations of cryptography [49]. The traditional key pre-distribution schemes lack its effectiveness in the up-scale network as well it poses higher memory overhead along with the vulnerable to the node capture attacks, a work of **Liu et al. (2008)** proposes a self-configurable mechanism to bootstraps the keys in up-scale WSNs. They claim by that time only this method archives resilience against node capture attacks along with the optimal scalability, storage and key-sharing probability [50]. An approach where the sink multicast the message to the nodes in a secure manner is an adopted service as multicast security. The multicast encryptions require attention to strengthen its efficiency for group-key distribution challenges. One the work by **Ren et al. (2009)** proposes a method where global partitioning and local diffusion is done to achieve these goals [51]. One another security service namely broadcast authentication where the mobile users broadcast message to the multiple sensor nodes. The traditional approach of symmetric key lacks the defensive capacity against the energy drain attacks and delays the message authentication process. The work by **Ren et al. (2009)** proposes PKC based method for broadcast authentication by exploiting Bloom filter, Signature, Merkle hash to achieve energy efficacy to compensate computation and communication overheads [52]. The WSNs stated adopting mobile sinks for many advantages but poses new challenges of security as attackers may compromise the by the acquisition of keys and gain control on the network just by deploying a cloned mobile sink. **Rasheed et al. (2012)** propose a scheme where two distinguished key pools are provisioned to strengthening the authentication process to mitigate the effect of mobile sink replication attacks which are proven to be better that polynomial pool scheme [53]. **Harn et al. (2015**) propose a novel redistribution method for group key by formulating a problem of multivariate optimization in RSA to be suited for WSN [54].

The use of complexed heavyweight encryption methods is not suitable for resource constrained WSNs. The work proposed by. **Zhao et al. (2017)** is a light weighted data aggregation using homomorphic encryption scheme [55]. Another approach where the compression is utilized the chaotic method for encryption and authentication is proposed by **Qi et al. (2015)** also uses compressed sensing to minimize the energy consumption to compensate security overheads [56]. The survey conducted by

Shim et al. (2016), concludes that The PKC can be categorized as 1) PKSc: RSA, ECC, 2) PKSs -Lattices and 3) PKCs with multivariate that makes the direction of cryptographic protocol development suitable for WSN security [57].

5. CONCLUSION

The wireless sensor network is useful network as a stand-alone network for many critical applications as well as a most basic sub-system of the Internet of Things (IoT). Therefore, achieving the security goal is one of the essential requirements to realize the seamless network quality of services (QoS). The use of customized elliptical curve, signature and encryption schemes is found quite often in the literature due to its suitability. The overall security requirements need both aspects to be covered one a proactive approach to the adoption of cryptographic approach suitable for the resource constraint context as well it requires security measures against both active and passive attacks. With the evolving architecture, applications of WSN the problem domain of security remains an open and active research issue which require an optimal solution.

6. REFERENCES

[1] T. Vladimirova, C. P. Bridges, J. R. Paul, S. A. Malik and M. N. Sweeting, "Space-based wireless sensor networks: Design issues," 2010 IEEE Aerospace Conference, Big Sky, MT, 2010, pp. 1-14

[2] A. B. Noel, A. Abdaoui, T. Elfouly, M. H. Ahmed, A. Badawy and M. S. Shehata, "Structural Health Monitoring Using Wireless Sensor Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1403-1423, third quarter 2017.

[3] C. Ioannou, V. Vassiliou, and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," *2017 24th International Conference on Telecommunications (ICT)*, Limassol, 2017, pp. 1-5.

[4] F. Walid and T. Ezzedine, "Design of a climate monitoring system based on the sensor network," *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, 2017, pp. 1791-1796

[5] T. Cao-Hoang and C. N. Duy, "Environment monitoring system for agricultural application based on the wireless sensor network," *2017 Seventh International Conference on Information Science and Technology (ICIST)*, Da Nang, 2017, pp. 99-102

[6] B. Stojkoska and D. Davcev, "Web Interface for Habitat Monitoring Using Wireless Sensor Network," 2009 Fifth International Conference on Wireless and Mobile Communications, Cannes, La Bocca, 2009, pp. 157-162.

[7] H. Elayan, R. M. Shubair, and A. Kiourti, "Wireless sensors for medical applications: Current status and future challenges," *2017 11th European Conference on Antennas and Propagation (EUCAP)*, Paris, 2017, pp. 2478-2482.

[8] T. Farnham, "Proactive wireless sensor network for industrial IoT," *2017 IEEE International Conference on Communications (ICC)*, Paris, 2017, pp. 1-6.

[9] H. Wu and M. Shahidehpour, "Applications of wireless sensor networks for area coverage in microgrids," 2017 IEEE Manchester PowerTech, Manchester, 2017, pp. 1-1

[10] M. Grabia, T. Markowski, J. Mruczkiewicz and K. Plec, "Design of a DASH7 low power wireless sensor network for Industry 4.0 applications," 2017 IEEE International Conference on RFID Technology & Application (RFID-TA), Warsaw, 2017, pp. 254-259

[11] Saha S., Bhattacharyya D., Kim T. (2010) OSI Layer Wise Security Analysis of Wireless Sensor Network. In: Kim T., Pal S.K., Grosky W.I., Pissinou N., Shih T.K., Ślęzak D. (eds) Signal Processing and Multimedia. Communications in Computer and Information Science, vol 123. Springer, Berlin, Heidelberg

[12] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, Protocols for Self- Organization of a Wireless Sensor Network, In IEEE Pers. Commun,7(5), 16–27, 2000.

[13] M. Tiloca, D. De Guglielmo, G. Dini and G. Anastasi, "SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks," *2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA)*, Cagliari, 2013, pp. 1-8

[14] M. M. Hossain, M. Fotouhi, and R. Hasan, Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, 2015 IEEE World Congress on Services, 21-28, 2015

[15] K. Xing, F. Liu, X. Cheng and D. H. C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," *2008 the 28th International Conference on Distributed Computing Systems*, Beijing, 2008, pp. 3-10

[16] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: A system theoretic approach," *49th IEEE Conference on Decision and Control (CDC)*, Atlanta, GA, 2010, pp. 6765-6772

[17] R. Di Pietro and S. Guarino, "Confidentiality and availability issues in Mobile Unattended Wireless Sensor Networks," *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile, and Multimedia Networks" (WoWMoM)*, Madrid, 2013, pp. 1-6

[18] K. Hameed *et al*., "A Zero Watermarking Scheme for Data Integrity in Wireless Sensor Networks," *2016 19th International Conference on Network-Based Information Systems (NBiS)*, Ostrava, 2016, pp. 119-126

[19] A. Taherkordi, M. A. Taleghan, and M. Sharifi, "Achieving availability and reliability in wireless sensor networks applications," *First International Conference on Availability, Reliability, and Security (ARES'06)*, 2006, pp. 7

[20] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, Dec. 2017

[21] S. Wu, B. Liu, X. Bai, and Y. Hou, "Eavesdropping-Based Gossip Algorithms for Distributed Consensus in Wireless Sensor Networks," in *IEEE Signal Processing Letters*, vol. 22, no. 9, pp. 1388-1391, Sept. 2015

[22] A. Proaño, L. Lazos, and M. Krunz, "Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 3, pp. 857-871, March 1 201

[23] M. Tiloca, D. De Guglielmo, G. Dini, G. Anastasi and S. K. Das, "JAMMY: A Distributed and Dynamic Solution to

Selective Jamming Attack in TDMA WSNs," in *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 392-405, July-Aug. 1 2017

[24] J. Heo, J. J. Kim, S. Bahk and J. Paek, "Dodge-Jam: Anti-Jamming Technique for Low-Power and Lossy Wireless Networks," *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, San Diego, CA, 2017, pp. 1-9.

[25] A. A. Bodkhe and A. R. Raut, "Identifying Jammers in Wireless Sensor Network with an Approach to Defend Reactive Jammer," *2014 Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, 2014, pp. 89-92.

[26] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "Tamper-aware authentication framework for wireless sensor networks," in *IET Wireless Sensor Systems*, vol. 7, no. 3, pp. 73-81, 6 2017

[27] F. R. Salmasi, "A Self-Healing Induction Motor Drive With Model Free Sensor Tampering and Sensor Fault Detection, Isolation, and Compensation," in *IEEE Transactions on Industrial Electronics*, vol. 64, no. 8, pp. 6105-6115, Aug. 2017.

[28] G. y. Duan, "A Study and Design of Multi-node Tamper-Resistant Web System Based on Ring Structure," *2010 International Conference on Parallel and Distributed Computing, Applications and Technologies*, Wuhan, 2010, pp. 416-419.

[29] S. D. Babar, N. R. Prasad and R. Prasad, "Countermeasure for intelligent cluster-head jamming attack in wireless sensor network," *2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Atlantic City, NJ, 2013, pp. 1-8

[30] I. Dbibih, I. Iala, D. Aboutajdine and O. Zytoune, "Collision avoidance and service differentiation at the MAC layer of WSN designed for multi-purpose applications," *2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech)*, Marrakech, 2016, pp. 277-282.

[31] D. Ismail, M. Rahman, A. Saifullah and S. Madria, "RnR: Reverse & Replace Decoding for Collision Recovery in Wireless Sensor Networks," *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, San Diego, CA, 2017, pp. 1-9.

[32] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," Hindawi Publishing Corporation, Journal of Sensors,2016

[33] Danyang Qin, Shuang Jia, Songxiang Yang, Erfu Wang, and Qun Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks," Hindawi-Journal of Sensors, 2016

[34] Yuanyuan Zhang and Marine Minier[1,] "Selective Forwarding Attacks against Data and ACK Flows in Network Coding and Countermeasures," Hindawi- Journal of Computer Networks and Communications, 2012

[35] G. Han, X. Li, J. Jiang, L. Shu and J. Lloret, "Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks," in *The Computer Journal*, vol. 58, no. 6, pp. 1280-1292, June 2015.

[36] W. Dong and X. Liu, "Robust and Secure Time-Synchronization Against Sybil Attacks for Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1482-1491, Dec. 2015.

[37] Chang Zhou and Ze Wang, "A Two Dimension detection to node replication attacks in mobile sensor networks," *2016 10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, Xiamen, 2016, pp. 63-69

[38] Rupinder Singh, Jatinder Singh, and Ravinder Singh,"WRH T: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks," Mobile Information Systems, 2016

[39] Eirini Karapistoli and Anastasios A Economides, "ADLU: novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks," *EURASIP Journal on Information Security, Vol.3, 2014*

[40] R. Yan, T. Xu and M. Potkonjak, "Data integrity attacks and defenses for Intel lab sensor network," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, 2015, pp. 721-726.

[41] S. M. Nam and T. H. Cho, "Improvement of energy consumption and detection power for PVFS in wireless sensor networks," *2014 Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, Singapore, 2014, pp. 129-134.

[42] Hui Song, Sencun Zhu and Guohong Cao, "Attack-resilient time synchronization for wireless sensor networks," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, Washington, DC, 2005, pp. 8 pp.-772.

[43] P. C. Geethu and A. R. Mohammed, "Defense mechanism against selective forwarding attack in wireless sensor networks," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, 2013, pp. 1-4.

[44] D. Buch and D. Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Network," *3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011)*, Bangalore, 2011, pp. 7-14.

[45] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor network security: a survey," in *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52-73, Second Quarter 2009.

[46] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. 2nd ACM International Conf. Wireless Sensor Networks Applications, 2003, pp. 151–159.

[47] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Springer Netherlands Wireless Networks, vol. 8, pp. 521–534, 2002.

[48] X. Huang, B. Chen, A. Markham, Q. Wang, Z. Yan and A. W. Roscoe, "Human interactive secure key and identity

exchange protocols in body sensor networks," in *IET Information Security*, vol. 7, no. 1, pp. 30-38, March 2013

[49] S. Sung and J. Ryou, "ID-based sensor node authentication for multi-layer sensor networks," in Journal of Communications and Networks, vol. 16, no. 4, pp. 363-370, Aug. 2014.

[50] F. Liu, X. Cheng, L. Ma and K. Xing, "SBK: A Self-Configuring Framework for Bootstrapping Keys in Sensor Networks," in *IEEE Transactions on Mobile Computing*, vol. 7, no. 7, pp. 858-868, July 2008

[51] K. Ren, W. Lou, B. Zhu and S. Jajodia, "Secure and Efficient Multicast in Wireless Sensor Networks Allowing Ad hoc Group Formation," in *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 2018-2029, May 2009

[52] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," in *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4554-4564, Oct. 2009

[53] A. Rasheed and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 5, pp. 958-965, May 2012.

[54] L. Harn and C. F. Hsu, "Predistribution Scheme for Establishing Group Keys in Wireless Sensor Networks," in *IEEE Sensors Journal*, vol. 15, no. 9, pp. 5103-5108, Sept. 2015

[55] X. Zhao, J. Zhu, X. Liang, S. Jiang and Q. Chen, "Lightweight and integrity-protecting oriented data aggregation scheme for wireless sensor networks," in *IET Information Security*, vol. 11, no. 2, pp. 82-88, 3 2017.

[56] J. Qi, X. Hu, Y. Ma and Y. Sun, "A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme," in *IEEE Access*, vol. 3, pp. 718-724, 2015.

[57] K. A. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, First quarter 2016.