International Journal of Computers and Applications

ISSN: 1206-212X (Print) 1925-7074 (Online) Journal homepage: http://www.tandfonline.com/loi/tjca20

Practical overview of security issues in wireless sensor network applications

Harish Radhappa, Lei Pan, James Xi Zheng & Sheng Wen

To cite this article: Harish Radhappa, Lei Pan, James Xi Zheng & Sheng Wen (2017): Practical overview of security issues in wireless sensor network applications, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2017.1398214

To link to this article: https://doi.org/10.1080/1206212X.2017.1398214

INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS, 2017
https://doi.org/10.1080/1206212X.2017.1398214

Practical overview of security issues in wireless sensor network applications

Harish Radhappa, Lei Pan, James Xi Zheng and Sheng Wen

Faculty of SEBE, School of Information Technology, Deakin University, Geelong, Australia

ABSTRACT

Wireless sensor networks are widely used in applications to monitor and communicate data. Even though the wireless sensor networks have been broadly used in critical applications, security and privacy issues are major concern. The attackers can gain considerably easy access into a wireless sensor networks and inject malicious data. Wireless sensor networks are considered to be vulnerable to the attacks. The aim of this research is to review the practical scenarios and applications, expose the security vulnerabilities and issues associated with wireless sensor networks specific to applications. The need for research in this area is high since it provides a broad scope to investigate problems and issues in current applications.

ARTICLE HISTORY
Received 16 March 2017
Accepted 26 October 2017

KEYWORDS
Wireless sensor network; two-phase hybrid cryptographic algorithm (THCA); symmetric cryptography; asymmetric cryptography

1. Introduction

Wireless sensor networks are a set of spatially distributed autonomous nodes over a large area that can cooperatively monitor and communicate the data to the central server through wireless network [1]. Sensor networks are being utilized in many areas, including environmental conditions monitoring, military application, tracking and monitoring animals, detection of harmful animals, smart buildings, structural health monitoring, automobiles, and so on. These wireless sensor networks are capable of detecting specific conditions, such as temperature, pressure, humidity, sound, motion of objects, pollutants. In every application, security is the fundamental factor, and mechanisms must be designed to have a secured environment.

1.1. Motivation

The survey in this context summarizes the application scenarios of wireless sensor networks. Here, we focus on three application scenarios – environmental wireless sensor networks, structural health monitoring, and smart building wireless sensor networks. And these three application areas are scaled to large-, medium-, and small-scale applications, respectively. The below Figure 1 shows the scheme of study.

We summarize and compare pros and cons for each application. Based on this analysis and comparison summarized, we briefly investigate the open issues. The investigations raise potential research questions and hence, it gave us strong motive to conduct broad research in this area.

1.2. Application scenarios

Wireless sensor network applications handle the sensitive data and important information, hence the wireless sensor networks are considered as critical systems. The wireless sensor networks are widely used to communicate and process data among the nodes. Over the last decade, the evolution of sensor network technology is at its peak where the applications developed focusing various operational areas. For the practical research ideology, the real-world scenarios are studied under three applications.

1.2.1. Environmental wireless sensor networks

Environmental wireless sensor networks is a broad research area and it is observed that environmental sensor networks as a large application has rapid development in recent years. In this applications category, spring brook rain forest which is one of the world heritage in Australia is considered as one of the motivating application and the security issues and vulnerabilities are studied in this context [2,3].

The spring brook rain forest is the long term and the large-scale monitoring wireless sensor networks. The wireless sensor networks of spring brook rain forest is the means for tracking the restoration of bio-diversity. The major responsibilities of wireless sensor networks on spring brook rain forest are temperature monitor, wetness of the leaves, speed of the wind, soil moisture, and direction of wind. It also includes the video monitoring along with the bio-acoustic technique [4–6]. The remote fire detection senses any fire incidents and is responsible

CONTACT James Xi Zheng james.zheng@mq.edu.au

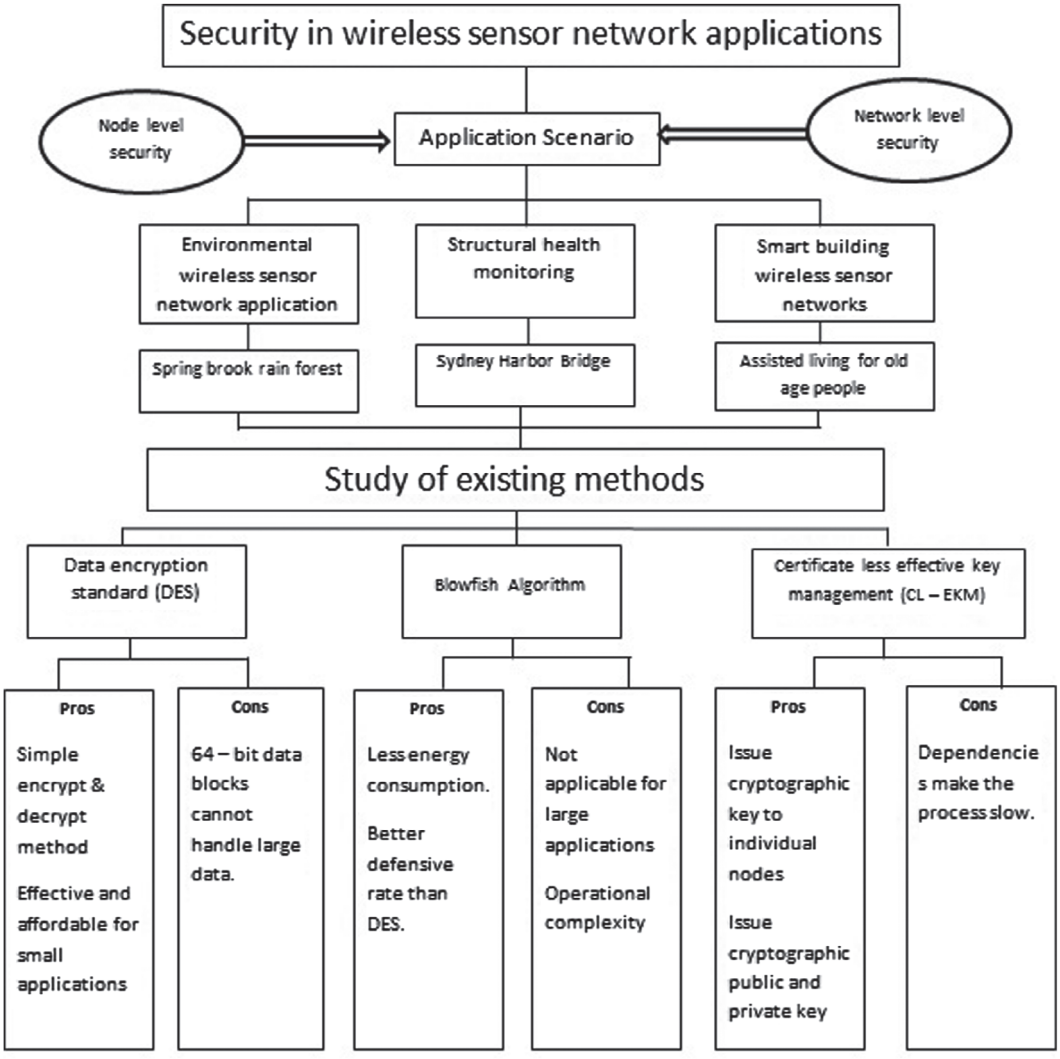

Figure 1. Study overview.

to raise an alert alarm and send it to the central server [5]. In these kind of large and mission critical applications the security threats and possibilities of intrusions are high, and there is a need for research to find expose the issues and aim to provide optimal security to the system.

1.2.2. Structural health monitoring

Structural health monitoring is another application which uses wireless sensor networks to detect the damage in the civil structures in an early stages [7]. Structural health monitoring is a continuous monitoring process, the health of any structure needs a thorough monitoring and accurately detect any damages to the structure. The SHM is a measure which is determined using accelerometer sensors. It is observed that performance and accuracy not only depends on the properties of sensors but also depends on wireless sensor network used for the acquisition of data and the transmission from the respective sensor node to the base station [8].

Some structural health monitoring applications are based on vibration detection mechanism [9–11]. This technique may be mainly used with structures, like bridges and tunnels. In this context we consider the project named 'Sydney Harbor Bridge', as a motivational paradigm. The bridge health, condition and serviceability needs a thorough monitoring [12]. This application is a medium-scale application.

There could be two strategies for monitoring the health of the bridge, firstly, direct damage detection and secondly indirect damage detection which actually focuses on the changes of dynamic structural properties. This requires dynamic cryptographic methods to have a secured communication which is discussed in the later sections in this context [10].

1.2.3. Smart buildings wireless sensor networks

The third application scenario is the smart building wireless sensor networks. Smart building wireless sensor net-

works are the small-scale applications. These applications are commonly used in small buildings and houses for personal or specific use. Smart building WSN's monitor and perform application-specific tasks in small areas. Here, we consider the project named 'Assisted living for old age people' as a motivational application [13].

The smart home-assisted living for old age people is capable to incorporate high computational powers to monitor the old age occupant activities and identify the required facilities and needs [14]. The wireless sensor networks are capable of integrating into a wide varieties of medical systems. Hence, the aging systems have induced significant interest in smart systems-assisting individuals.

In the above-mentioned motivation applications, the real-world security attacks may not reveal from respective agencies, but an article by Brix [15] explains the future scenario of wireless sensor network applications. The article states that, the small-scale sensor networks such as smart homes could be easily attacked by gaining access to various devices at the house such as security alarm, motion detectors door control [15]. At the same time, author mention that the learning curve between scientists and engineers such that engineers and architects may have immense efforts towards security measure but the research proves even today the security measure is not sufficient [15].

The study explains scenarios of each case, ranging from small scale to large area applications. Due to the security issues from the above motivating applications, the security aspects are analyzed in the further sections.

2. Problem statement

Since wireless sensor networks are no more deployed in an enclosed environment, they are vulnerable to attacks and intrusions. The potential issues associated with wireless sensor networks are:

- Nodes may process unsolicited information either by accident or purposefully injected by the attacker.
- Since capacity of wireless sensor nodes are limited, scalability is a concern during large data processing.
- Security at network level in current scenario has a larger focus, but security at node level needs an equal importance.
- Basic sensor network applications are economical and can be affordable for small purposes but are vulnerable to attacks.
- Advanced large-scale applications are secure to an optimal extent but are very expensive.

The end results of the survey expose the vulnerabilities of wireless sensor network applications from multiple dimensions. The study over various wireless sensor network applications can be classified into three levels as shown in Figure 2.

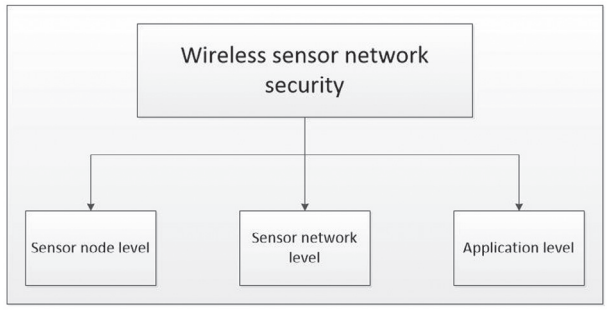

Figure 2. Classification of levels.

Based on the above classifications, the applications are studied which includes the major contributions as below:

- Investigate and expose the security issues.
- Identify application vulnerabilities, both at node level and network level.
- Identify existing mechanisms of intrusion detection system, analyze level of accuracy and performance.
- Prioritize the issues based on level of risk and identify security requirements with respect to wireless sensor networks.

3. Related work

Wark et al. [16] expose the transport layer attacks which can be like desynchronization and flooding. In this layer, the attacker breaks through the authentication and be a man in the middle tampering the data packets [16]. The main advantage with wireless sensor networks is their easy deployability, but in contrast, the disadvantage is that wireless sensor networks in an ad-hoc environment are vulnerable to attacks against various parameters [17]. In spite of above-mentioned diverse nature of wireless sensor networks, the encryption and aggregation imposes scalability problems to wireless sensor networks.

The study by Butun et al. [18] on security vulnerabilities in sensor networks expose lack of physical layer defense [18], having security as the major concern the focus in this context is partly based on confidentiality. The study look forward to detect any kind of intrusions or malicious signals way before attackers can cause any damage to the network. The study shows detection of both internal and external intruders [18].

Faults and failures commonly occur in wireless sensor networks. Mahapatro and Khilar [15] survey article is about diagnosis of faults and failures in WSN's. Due to continuous changes in surrounding conditions and environmental hazards, the wireless sensor networks are prone to failures [15]. The author observation shows frequent and unexpected occurrences of faults and failures

under specific conditions. The objective of this study is to expose the diagnosis techniques of faulty sensor nodes in wireless sensor networks.

Illiano and Lupu [19] Survey is based on detecting the intruder data injections. Once a node or a communication channel is attacked, there could be malicious data introduced in the network. This is called as data injection. The survey reviews the approaches and mechanisms in data injection. The limitations identified in this study are frequent node failures, lower redundancy, and fewer capabilities in handling the complex data [19]. WSN's have high risk of compromising nodes towards intruders. The detection of malicious data can be classified mainly into two approaches, namely anomaly detection and trust management [19–24]. These approaches are analyzed and compared by their respective definitions of expected behavior. Also the study addresses two aspects, namely 'diagnosis' and 'characterization'. Diagnosis is a method of identifying the root cause of anomalies. Characterization is used to detect the compromised nodes [19]. But a further study and investigation is required with respect to attack characterization and identify the compromised nodes during high data traffic and collusion.

Mansour et al. [25] is a study based on key management in wireless sensor networks. The study reviews the revoking and keys renewal in avoidance with the malicious nodes. The authors propose a secure key management mechanism based on symmetric encryption and the proposal is based on the technique called elliptic curve cryptography [25]. Authors consider every protocol to be secure by default but it is not that they are not fully secure, the level of security depends on various factors. The study shows that asymmetric encryption methods cannot be directly used on sensor nodes due to the resource constraints. This mechanism overcomes the disadvantage of random key pre-distribution, since probability of sensor nodes to choose the similar keys, the attacker can capture node easily which leads to exposure of all encryption keys to the attacker from the captured node. Hence in the proposed key revoke mechanism a periodical key certificates are created, hence eliminating key duplication [25].

George and Parani [26] study is based on detection of clones in a wireless sensor networks. Cloning attack is a condition where the attacker behaves as one of the actual node by disguising. Cloning or impersonation attacks could be fatal in wireless sensor network applications. The cloning usually takes place in medium-scale and small-scale applications. If an attacker could perform this attack the target node could lose the critical data and also consequences could be impersonation of entire hardware. Cloning attack usually takes form of tampering attack in a sensor network [26]. A distributed hash table approach provides decentralized scheme along with checking of the keys from hash table. The detection may be initiated by sending a request by initiator. Distributed hash table contains the entire records of key pairs distributed to the genuine nodes [26]. This technique basically eliminates the unauthorized data access. The main strength of the proposed algorithm is that the multi-identifications from the attacker could be identified which is basically termed as Sybil attack. The main weakness or drawback of this technique is that the detection would take place once the probabilistic data are shared with the destination. Having neglected Sybil attack at later stages may lead to loss of data and impersonation as the attacker would have gained entire access to the network.

Ren et al. [27] study is based on broadcast authentication which is considered to be a critical service in wireless sensor network application [27]. Broadcast of data with authentication is a secured way of data transfer from source to destination. Denial of Service (DoS) attacks are common in this context due to delay in authentication. The author proves that cryptographic techniques such as Merkle hash tree, identity signature scheme are all computationally expensive and also create communication overhead [27]. Hence, the author provides the quantitative analysis in this context. The author proposes a certificate based authentication technique which makes use of both public key as well as private key pair. Every message that broadcast is appended with signature. To prove the authenticity the sink is also assigned a public key and a private key. These is a two-way handshake mechanism authentication scheme. The strength of this technique is that every node verifies the data in two stages, and authorized user need not require certificate to prove the public key binding. The weakness of the application is that it fails to explain the scenarios in case of multiple broadcast authentication.

4. Security vulnerabilities, issues, and attack analysis

Security is the primary concern in a wireless sensor network. For the wireless sensor networks to be secure, there are few requirements to be satisfied. These requirements are commonly applicable to all the three motivating applications mentioned before.

(1) Secure authorization is one of main requirements since only the authorized sensor nodes should be able to have the access to the network.
(2) The identities must be verifiable of any message and respective nodes in a network. It should be

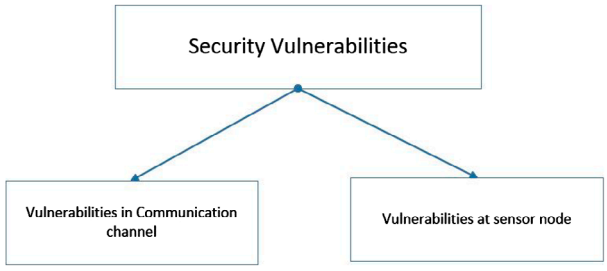

Figure 3. Classification of security attacks in wireless sensor networks.

impossible for the attackers to forge the data which can be indistinguishable between benign and malicious data.

(3) The meta-data which is required for network purposes must be concealed to everyone, this might include even the network authorities.
(4) Data and information stored on flash memory of a node should not supposed to be divulged under any given conditions to the attackers or unauthorized personnel.
(5) The privacy and confidentiality of data in a network must not be breached at any point of time. In case of above small-scale motivating application, it contains personal data of old age people, and such data needs privacy and need to be confidential.
(6) The sensor network services must be available all the time and should not be vulnerable to DoS attacks. Also the availability if a service in the network even during system failure and malfunction is an important aspect.
(7) Resistance towards DoS attacks is a critical requirement. Since the all the three motivation applications from above are vulnerable to DoS attacks.
(8) The newness of the message must be possible to be verified all the time and in every application during the data exchange which can prevent the reuse of any older data by the attacker.
(9) The protocol needs to be resilient towards node compromise attacks. Small-scale applications are very vulnerable to node compromise attacks.

The modern wireless sensor networks communication is through radio signals between the physical sensor nodes and sink. Hence, the communication in WSN's rely on sensor node ability to form an ad-hoc multi-hop radio network. In current world, wireless sensor networks several security vulnerabilities can be identified. We study and classify vulnerabilities as shown in Figure 3.

Vulnerabilities in communication channel may mainly occur in between two sensor nodes communication. The transmitted information from the sensor node may be eavesdropped and malicious data may be injected by the intruder and replay it in the network, this is possible even without having any actual physical access to any of the sensor nodes or the components in the network.

The eavesdropping could occur during the attacks against confidentiality and privacy. Whenever the end to end security measures fail in a network, an attacker can possibly discover the network contents by eavesdropping on the frequency of the particular network. This kind of attacks may be possible mainly with small-scale and medium scale-applications mentioned above. Here in this context, say if the sensor networks deployed in an assisted living for old age people can be eavesdropped then the victim (for example, an old age person) health records pertaining to the heart rate, activities and motions could be accessed by the attacker and malicious data can injected to create a false data in the records.

Vulnerabilities of sensor nodes are subject to physical layer attacks. The wireless sensor nodes are generally prone to attacks such as tampering and node capture attacks. When an attacker can gain access to any of the sensor node in a network then attacker can perform the following actions [28]:

- Information theft (Sensitive data).
- Reprogramming the nodes to alter default behavior.
- Damage the senor nodes physically and terminate the node services.

At the node level security, another concern is the security to the memory. In the modern wireless sensor networks there is a small amount of flash memory on every sensor node to store the temporary data before transmission. This temporary memory size vary in small applications to large applications. In a large applications like environmental monitoring there is an interval of time to transmit the data to the base station, but the data to a certain amount of time is stored on the sensor node. Similarly with medium-scale and small-scale applications, the data would be temporarily stored on sensor node for a short period of time. If the attacker could gain the access to this memory, the critical could be changed in the memory before transmission. Taking an instance from above motivation applications, if a temperature log is stored in the memory for a certain time and if the attacker could gain access to the particular node, then temperature log could be altered to show false results hence, might create even false emergencies in that locality.

Figure 4 shows how security attacks in wireless sensor networks are classified. We classify the attacks with various layers of wireless sensor networks. There could be other kinds of attacks but according to the motivational application vulnerabilities these attacks are considered in this context.

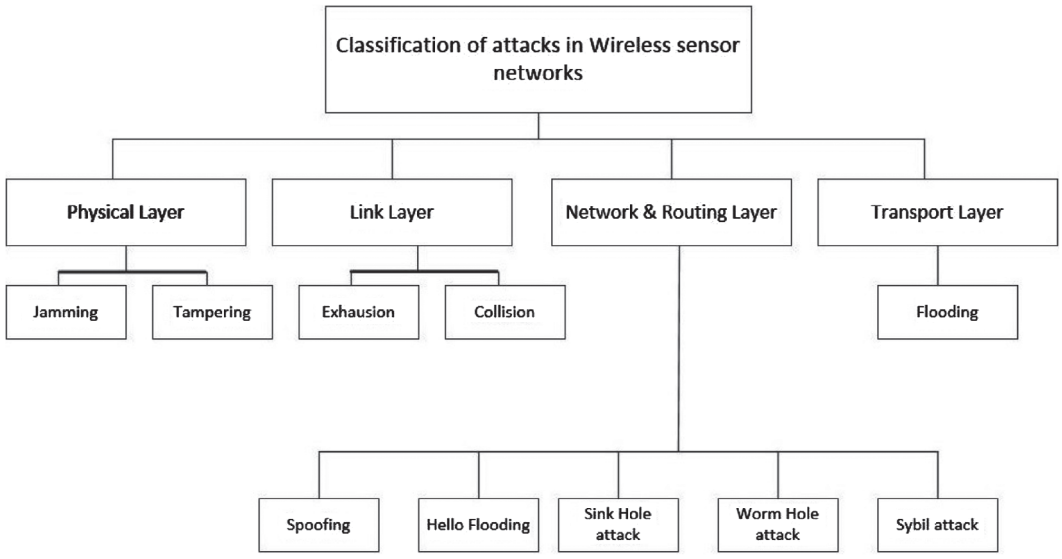

Figure 4. Classification of vulnerabilities.

4.1. Physical layer attacks

In this layer, the attacks can be on either sensor nodes or with the communication channel. Physical layer attacks focus the target with small-scale applications and medium applications since these contain mission critical data.

4.2. Link layer attacks

The attacks in this layer are similar to that of physical layer. The intrusions may happen through the radio signals and manipulation of efficiency measures in a protocol. This can cause the expense of additional energy drain bringing down entire network to an inactive state. The protocol vulnerabilities occur in every application, but ranges the severity from small to large.

4.3. Network & routing layer attacks

In this layer, many kind of attacks are available to disrupt the network. Security at the network level mainly depends on authentication techniques. Wireless sensor networks are resource constrained and hence, the public key cryptography is not feasible for small-scale wireless sensor networks. The symmetric keys and hash functions can be best suited for small-scale and medium-scale applications. However for large applications like spring brook rain forests, the potential network threats are higher and hence, sophisticated cryptographic methods may be used [29]. The network and routing layer attacks commonly occur in all kinds of applications, since most of the attacks is with aspect of communication the attacker would be an outside attacker, hence large, medium and small applications are all vulnerable to network and routing layer attacks.

4.4. Transport layer attacks

The transport layer protocols provide congestion control mechanisms and reliability [30] during the transfer of data. Providing security and authentication to the transmission protocols in this layer can solve various issues. All the above-mentioned three motivational applications are vulnerable to above-mentioned attacks, respectively. But this is commonly applied to the large-scale applications as they are observed to have larger standby data for a certain period. Hence, attackers would mainly target large applications with this technique. The medium-scale applications have reasonably high threat from transport layer attacks but depends on time periods of data transmissions a medium-scale applications could possess.

According to the study in this context, from the above-mentioned three motivating applications, the large-scale spring brook rain forest application and medium-scale Sydney Harbor Bridge Structural Health Monitoring basically use IPv6 protocol for remote communication [31]. The IPv6 protocol is used for communication over the Internet when the gateway or sink at remotely located from the physical location of wireless sensor networks. Hence in case of above-mentioned two applications, the remote communication takes place using IPv6 [31]. Conventionally, many of such applications run using IPv4. The reason behind the replacement of IPv4 with IPv6 is that, IPv4 is observed to provide relatively less address space. But this was overcome by IPv6 which was capable

of supporting upto 3.4×10^{38} addresses [31]. This is observed to be nearly 7.9×10^{28} times more when compared to IPv4.

Even though IPv6 provides many advantages, it would also potentially raise security issues. It is observed that IPv6 protocol is more vulnerable towards wormhole attacks, where attacker can use expansion headers in damaging entire IPv6 network.

5. Existing solutions

In previous sections, the security vulnerabilities and issues are exposed based on three motivational applications. In this context, we consider few existing solutions and analyze their applicability and accuracy in solving current research issues pertaining to the three motivational applications mentioned above. Intrusion detection systems cannot alone provide security, and also intrusion detection systems are capable of identifying the intrusions and raise and alert upon identifying any malicious activity. Protecting the wireless sensor networks from attacks is out of capabilities of IDS, since IDS are capable of only detection and monitoring part of security. So in order to prevent malicious attacks and intrusions in a wireless sensor network, we need cryptographic methods.

The standardized approach towards security is cryptography [32]. The data would be encrypted and sent over the network and hence only authorized personal could decrypt the data. Symmetric key cryptographic is a well-known technique used for data authentication and confidentiality in a wireless sensor network. For medium-scale and small-scale applications like structural health monitoring and smart home systems, the simpler cryptographic methods could be feasible such as one way hash functions and also the effective and efficient symmetric schemes adds optimal security in any application [33]. In case of larger sensor network applications, such as environmental monitoring wireless sensor networks – 'spring brook rain forest', due to its large application area and wide spread nodes the communication takes place over a large distance. Hence, a stringent security is required such as public key cryptography.

Here on first hand, we consider DES and blowfish algorithm [34], propose cipher block chaining (CBC) and use the above-mentioned techniques to derive an efficient solution. This is an application specific security mechanism designed for environmental systems which monitor temperature, pressure, sound, etc.

5.1. Data encryption standard

Data encryption standard (DES) is a block cipher encryption technique. It contains a 64-bit block of data with key of 56 bits. The DES operates in three stages as mentioned below:

- Permutation on 64 bits generating the permutation input.
- Then followed by 16 rounds of iteration of function with random keys in every round, also with a pre-output.
- Final stage is the inverse permutation to obtain desired cipher block.

The above steps show the encryption part of DES, and decryption part is a simple step where sub keys are reversed [34]. This technique would fail to provide optimal security for large applications, however, this would be fairly a feasible solution for medium-scale applications.

5.2. Blowfish algorithm

Blowfish is also a symmetric key block cipher. It also contains 64-bits block of data and size varies with 448 bits. The blowfish algorithm is considered to be Feistel Network which is also having the 16 iterations of encryption function. The major feature of this technique is that a complex key schedule actually makes the algorithm much stronger. The encryption in blowfish technique is such that data blocks of 64-bit is subdivided into two halves of 32- bits each. The sub- parts consists of an 18-bit entry, a p-array and a 256-bit entry S-box. These S-boxes maps the inputs of 8 bits into a 32-bit output. At least one single entry of p-array is mandatory for every round. And remaining p-array may be used after final iteration in XOR outputs in each half. Unlike DES, the blow fish decryption is the same reversal procedure. Blow fish algorithm with cipher block chaining is applicable for small-scale and medium-scale applications. Given the comparison, this technique is more feasible and can provide better security for small-scale applications than the DES. And similar to DES, even this technique would fail to reach the standards for large-scale applications and considered to be a moderate solution in case of medium-scale applications.

5.2.1. Cipher block chain

CBC is the block operation mode to generate blocks of ciphers which is 64 bits. The CBC vector initialization is used with first block text and subsequent blocks are XOR with previous cipher block before encryption. And decryption is done after decrypting the cipher block. The CBC has a limitation where the algorithm restricts the parallel encryption, which means the process of encryption does not proceed forward until the previous blocks are encrypted. Hence, there exist a dependency.

The capability of CBC in conjunction with DES or blowfish is observed to have optimal data confidentiality

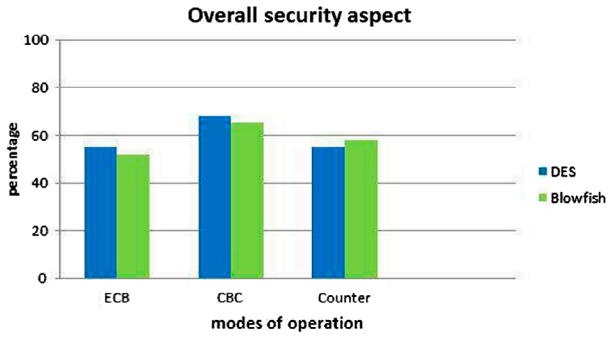

Figure 5. Security aspects DES vs. Blowfish. Source: (24).

and security in the network. And algorithm is observed to be hard to break through by the specific intruders in case of specific applications. The capacity in generating secure encrypted packets can be observed in cipher bloc chaining with Blowfish algorithm. Compared to DES the blowfish algorithm is harder to break through security compared to normal stream ciphers. Figure 5 is the analytical results from G. Kumar et al. [34] which shows the overall security aspects comparison.

5.3. Solution to node level security

There are several approaches in the context of compromised nodes, but these approaches can be categorized into two parts [21,22]. The first category approach is detection of false information and tolerance of data injected by the intruders specifically during data aggregation [21]. In this approach, the validity of data are checked through sampling mechanism at the base station. But major disadvantage with the current approach is that, it cannot be used to determine the root cause of the attack.

The second approach basically deals with application specific mechanism, here every single node is responsible to monitor the activities of neighboring nodes [24]. Any activity observed to be abnormal, then an alert signal is raised to corresponding neighboring nodes or to the sink [24]. Localized alert-based mechanism is an extended study to this approach [23]. Any signal trigger from any of the sensor node in the network can point out compromised node. Even in this mechanism, it is an ambiguous situation if the alert can be trusted or not. Since the compromised nodes are capable of raising the false alerts which might mislead the network traffic and gateway [18,20–23,35].

Zhang et al. [35] propose a framework in identifying compromised nodes in sensor networks. The framework focus on independent applications and provide an abstract level of detection mechanisms. The framework proposed [35] is an application-independent framework to identify the compromised nodes. The structure of framework is such that, centralized component is responsible for relative monitoring of neighboring sensor nodes. This architecture also determines the accuracy in detecting the compromised node. The designed algorithm may not rely on any assumptions towards behavior of sensor nodes in a network, but the algorithm is only capable of identifying major amount of compromised nodes that generate false alerts without the introduction of the false positives. The experiment limits itself to 200 nodes [35], but there is no information of dynamic applicability of algorithm to large amount of nodes. And the drawback identified in this context is that algorithm may fail to identify the compromised nodes in case of multiprocessor systems.

5.4. Certificate less effective key management

The structural health monitoring – Sydney Harbor Bridge and Assisted living for old age people are medium-and small-scale applications, respectively. These applications are dynamic in nature, which means the sensor nodes may leave or be added to the network dynamically. The key security requirements of this dynamic nature wireless sensor networks are confidentiality, integrity and sensor node authentication. Conventionally symmetric key encryptions [36,37] were used for majority of encryption key management protocols. But for the dynamic applications, like structural monitoring and assisted living for old age people symmetric key encryption may not be feasible due to the limited resources and comparatively lesser processing capabilities. In case of symmetric key encryption, it needs large amount of memory space and also it suffers from communication overhead. Hence keeping this in view, a key management technique in dynamic nature is studied in this context. Seo et al. [38] propose a technique called certificate less effective key management (CL-EKM) for dynamic nature of wireless sensor networks. This technique basically supports the efficient cryptographic key updates when a sensor node leaves or joins the network. This technique also ensures the forward and backward key secrecy. This technique is efficient towards the node compromise attacks. By efficient key revoke mechanism for compromised nodes, the impact over security due to node compromise is reduced.

This technique makes use of two other basic algorithms, namely certificate less public key cryptography and a key generation center. This is a hybrid model of private and public key pairs which successfully removes the need for certificates. To establish secure communication between the nodes, the pair-wise key is shared between the nodes, and CL-EKM issue a certificate less hybrid signatures. This algorithm also supports light weight information processing consuming lesser node memory.

Key update functionality would be executed whenever a node moves out of network or gets added newly into the network, and key revocation would eventually be active when a malicious node is identified in a network. The small drawback of this technique is that it depends on IDS to raise an alert before key revocation process hence, its dependency over identification phase makes the process slower. This technique can be applicable for all the above-mentioned motivational applications but due to weakness of this method such as data forgery vulnerability, key compromise attacks this method is observed to be in – feasible under certain conditions. Hence there could be an enhancement with this technique which can be generally applicable for all applications.

6. Recommendations and proposals

The above three motivational applications vary in size and properties based on their area of functionality, but the underlying mechanisms in every sensor network application is nearly similar. Considering the node level security, the entire node level security depends on cryptographic keys. The authentication and access privileges need to be handled in order to restrict the attackers from accessing the sensible information on the node memory. Every time during the detection of compromised nodes only limited set of nodes with their compromised keys can be detected due to false detection ratio. Hence, efficient cryptographic mechanism along with intrusion detection can solve the problem. In this section, a possible cryptographic method is proposed to provide a generalized solution to security vulnerabilities is wireless sensor network applications. Also, we compare the above obtained solutions to check feasibility of each solution and effectiveness specific to the three motivational applications.

In the above discussed solution, symmetric key encryption alone cannot provide optimal security measures in a network. A hybrid model is proposed by Rizk and Akaldy [39], this is a hybrid model of symmetric and asymmetric cryptographic techniques. This method is called as 'Two-phase Hybrid Cryptographic Algorithm (THCA)'. This is a hybrid model combining the properties of four major cryptographic algorithms. It includes elliptical curve cryptography along with another standardized algorithm called advanced encryption standards (AES) together provide the encryption. The advanced version of RSA algorithm which is termed as 'XOR Dual RSA algorithm' is used for data authentication as well as sensor node authentication. And message digest 5 (MD5) technique is induced for providing the data integrity.

The THCA algorithm is a new efficient technique which combines symmetric and asymmetric techniques. In this method initially, the data are divided into 'n' blocks. Each block comprises of 128 bits. Another feature if this algorithm is that if 'n' is a non-integer and has only fraction part it automatically uses padding to nullify the last bit with 128 bits [39].

Unlike other algorithms, this technique has a unique encryption and decryption process. The encryption is divided into two phases. Each phase functionality is as follows:

Phase 1: The n/2 blocks would be encrypted using hybrid encryption algorithm (AES, ECC). ECC is responsible for protecting the secret key. AES is responsible to produce optimal system performance with low power consumption and minimal memory requirement.

Phase 2: This phase is also carried out in parallel with phase 1 in order to provide maximum level of security without increase in processing time. Further, the blocks are encrypted with XOR-Dual RSA which is extremely fast process. This method uses same key for both encryption and decryption.

Like encryption, the decryption side *Q* is also divided into 'n' blocks of 128 bits. The Hash function is used to verify the sink node if it has received exact cipher text. Here extensively the Hash values are compared from both the entities, if there is a match then decryption process is further proceeded else it would be discarded. Even the decryption process go through two phases. It is not the reverse way of encryption but it involves thorough decryption in every stage.

Having such a complex encryption and decryption methodology in least turn around time, it is feasible to be applied on to the wireless sensor network applications to obtain optimal security. Hence, this technique is acknowledged and proposed in this context as a feasible solution to the vulnerabilities and flaws mention in the previous sections. It takes a major advantage with respect to resource utilization, memory consumption on sensor nodes and limited power consumption along with fast and secure processing when compared to above existing solutions.

From the Table 1 comparison, we can observe that THCA is very efficient in case of large applications and medium applications. But due to resource constraints and limited resources in small-scale applications THCA would not be a feasible solution, because deploying THCA in small scale would impose resource utilization overhead, hence DES or the Blowfish algorithms with cipher block chaining would be best suited for small scale applications.

Along with cryptographic methods, in above sections, we have discussed and compared the intrusion detection systems in various scenarios. These intrusion detection

Table 1. Comparisons of solution based on above analysis.

Applications	Large scale motivation application			Medium scale motivation application			Small scale motivation application		
Solution set	DES – CBC	Blow Fish – CBC	THCA	DES – CBC	Blow Fish – CBC	THCA	DES – CBC	Blow Fish – CBC	THCA
Security against attacks	Low	Low	High	Moderate	Medium	High	High	High	High
Defence/Tolerance	Low	Low	High	Medium	Medium	High	High	Medium	High
Compatibility/Applicability	Medium	Medium	High	Medium	Medium	High	High	Medium	Low
Scalability	Medium	Medium	High	High	High	High	High	High	Low
Feasibility	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Coverage	Medium	Medium	High	Medium	Medium	High	High	High	Low
Memory utilization	Medium	Medium	Medium	Medium	Medium	High	Medium	Medium	High
Learning curve	Low	Low	High	Medium	Medium	High	High	Medium	Medium
Processing time	High	High	Less	High	High	Medium	Medium	Medium	N/A
Performance	Low	Low	Medium	Medium	Medium	High	High	High	Medium
Cost	Economical	Economical	Relatively affordable	Economical	Economical but affordable	Moderate	Economical expensive	Economical	Considerably

systems and cryptographic methods are very crucial in a wireless sensor network applications security. Based on the motivational application view, the cryptographic methods would effectively handle the attacks from all four layers. The level of complexity in every aspect increases as we go through small-scale applications like assisted living for old age people up to the large application spring brook rain forest. The area and number of sensor deployed in each motivation application varies but the security vulnerabilities and attacks are exposed based on complexity of a wireless sensor application.

7. Conclusion

The modern wireless sensor networks are deployed in a non-enclosed environment. Due to this nature of wireless sensor networks, many security issues arise and hence, wireless sensor networks are vulnerable to attacks. In this report, we consider three application scenarios and security vulnerabilities are exposed based on these applications. This report studies various aspects associated with security issues in wireless sensor networks. The key findings in above research indicate that wireless sensor networks are used in mission critical applications. At the same time, security issues in wireless sensor networks are also equally high.

In this study, we had a thorough analysis with existing solutions which mainly account for security vulnerabilities. The study on cryptographic methods and intrusion detection mechanisms are thoroughly analyzed and acknowledged in this context. Intrusion detection systems are responsible in identification of possible intruders and cryptographic methods play a key role in prevention of attacks. Hence for this purpose, we need an efficient cryptographic system. Since wireless sensor networks are resource constrained, the methodologies need to be feasible and best suited to provide optimal security with minimum resource utilization.

The discussed methodologies may not be feasible to every application scenario in this context. Even with the current solutions being enhanced, there are open issues which are listed below:

- Highly secured encryption and decryption algorithm can be complex at individual nodes. When these cryptographic algorithms applied on individual nodes can have higher resource utilization and processing time. This issue requires greater focus.
- Having a scalable and reliable solution which can provide security from small-scale applications to large-scale applications is one of the open challenge as studied in above application scenarios.
- The application scenarios portrait vulnerabilities with small and medium applications. Having a cost effective and efficient security mechanism in both the scenarios remains open issue with respective applications.

Considering the application scenarios the solutions are studied and recommendations are provided in this context as to which solution is best suited for each application. As we have seen above two-phase hybrid cryptographic algorithm (THCA) is a kind of solution which is expected for large-scale and medium-scale applications and the comparison table proves the reason behind it. And for small applications due to extreme resource constraints THCA is not feasible, as a result the DES or Blowfish algorithm with CBC is recommended. However these solutions are applicable with the limitations, the open issues listed above requires further research to optimize and overcome the limitations in the current methodologies.

Research challenges in wireless sensor networks depends on the application environment. In the current scenario, the new kind of attacks which are referred as timing attacks is a major research focus which is aimed to be studied as a future work in wireless sensor net-

works. Also in future, this research would focus on cache effects and its security vulnerabilities in a wireless sensor networks.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Harish Radhappa is a master's of IT student of Deakin. His research interest is in cyber security.

Lei Pan is a senior lecturer in the school of IT with Deakin University, Australia. He serves as a course director for cyber security discipline. He has a strong passion in teaching and researching cyber security problems and issues affecting the twenty-first century digital future. He has published more than 50 internationally peer-reviewed journal and conference papers. He is also an active educator on http://futurelearn.com/.

James Xi Zheng got PhD in Software Engineering from UT Austin, master's in Computer and Information Science from UNSW, bachelor's in Computer Information System from Fu-Dan. He was the chief solution architect for Menulog Australia and served as solution consultant for a few top 500 corporations, now assistant professor/lecturer in Software Engineering at Macquarie University, Australia. James Xi Zheng specialized in Service Computing, IoT Security and Reliability Analysis. He published more than 30 high-quality publications in top journals and conferences (PerCOM, ICSE, ICCPS, IEEE Systems Journal, ACM Transactions on Embedded Computing Systems, IEEE Transactions on Vehicular Technology. He is awarded the best paper in Australian distributed computing and doctoral conference in 2017 and the Deakin Research outstanding award in 2016.

Sheng Wen is a senior lecturer in the school of IT with Swinburne University of Technology, Australia. He serves as editor for a few top journals and his research interests are social networks, machine learning, and propagation modeling.

ORCID

Harish Radhappa http://orcid.org/0000-0001-9975-4694
Lei Pan http://orcid.org/0000-0002-4691-8330
Xi Zheng http://orcid.org/0000-0002-2572-2355

References

[1] Davis A, Chang H. A Survey of wireless sensor network architectures. Int J Comput Sci Eng Surv. 2012 Dec;3(6):1–22.
[2] Corke P, Jurdak R, Hu W, et al. Environmental wireless sensor networks. Proc IEEE. 2010;98(11):1903–1917.
[3] Othman MF, Shazali K. Wireless sensor network applications: a study in environment monitoring system. Procedia Engineering; 2012;41:1204–1210.
[4] Sha K, Shi W, Watkins O. Using wireless sensor networks for fire rescue applications: requirements and challenges. In: Proceedings of IEEE International Conference on Electro/information Technology; Orlando; 2006. p. 239–244.
[5] Jadhav PS, Deshmukh VU. Forest fire monitoring system based on ZIGBEE wireless sensor network. Int J Emerg Technol Adv Eng. 2012;2(12):187–191.
[6] Department of Environment and Resource Management. Springbrook wireless sensor network [Online]. Available from: https://springbrookrescue.org.au/WSN_brochure.pdf Accessed: Sept. 11, 2017.
[7] Runcie P, Mustapha S, Rakotoarivelo T. Advances in structural health monitoring system architecture. In: Proceedings of the Fourth International Symposium on Life-cycle Civil Engineering, IALCCE. Vol. 14; Tokyo; 2014.
[8] Raju KS. Implementation of a WSN system towards SHM of civil building structures. In: IEEE Sponsored 9th International Conference on Intelligent Systems and Control; Coimbatore, India; 2015. p. 1–7.
[9] Nguyen VV, Dackermann U, Li J, et al. Damage identification of a concrete arch beam based on frequency response functions and artificial neural networks. Electron J Struct Eng. 2015;14(1):75–84.
[10] Pakzad SN, Rocha GV, Yu B. Distributed modal identification using restricted auto regressive models. Int J Syst Sci. 2011;42(9):1473–1489.
[11] Brooks MJ, Dick AR, Van Den Hengel A. Towards intelligent networked video surveillance for the detection of suspicious behaviours. New Scientist. 2003;4.
[12] Nagayama T, Spencer BF. Structural health monitoring using smart sensors. Newmark Structural Engineering Laboratory. University of Illinois at Urbana-Champaign; 2007. Availabel from: https://www.ideals.illinois.edu/bitstream/handle/2142/3521/NSEL.Report.001.pdf?sequence=4 Accessed: May 19, 2017.
[13] Srinivas N, Reddy KS, Evuri GR. >Wireless sensor network based smart home for elder care. Int J Eng Sci Invention Res Dev. 2014;I(VI):1.
[14] El-Basioni BMM, El-Kader SMA, Eissa HS. Independent living for persons with disabilities and elderly people using smart home technology. Int J Appl Innov Eng Manage. 2014;3(4):11–28.
[15] Brix L. Your household appliances can be hacked [Online]; 2012. http://sciencenordic.com. Available from: http://sciencenordic.com/your-household-appliances-can-be-hacked Accessed: Sept. 12, 2017.
[16] Wark T, Hu W, Corke P, et al. Springbrook: challenges in developing a long-term, rainforest wireless sensor network. In: International conference on Intelligent Sensors, Sensor Networks and Information Processing; Sydney; 2008. p. 599–604.
[17] Di PR, Guarino S, Verde NV, et al. Security in wireless ad-hoc networks – a survey. Comput Commun J. 2014;51:1–20.
[18] Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE Commun Surv Tutorials. 2014;16(1):266–282.
[19] Illiano VP, Lupu EC. Detecting malicious data injections in wireless sensor networks: a survey. ACM Comput Surv. 2015;48(2):24:1–33.
[20] Rajasegarar S, Bezdek JC, Leckie C, et al. Elliptical anomalies in wireless sensor networks. ACM Trans Sens Netw. 2009;6(1). Article 7, 28 p.

[21] Du W, Deng J, Han YS, et al. A witness-based approach for data fusion assurance in wireless sensor networks. In: Proceedings of the IEEE Global Communications Conference; San Francisco; 2003. p. 1–5.
[22] Przydatek B, Song D, Perrig A. SIA: secure information aggregation in sensor networks. In: Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems; Los Angeles; 2003. p. 255–265.
[23] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks. ACM Trans J. 2005;20:1–35.
[24] Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Trans Sens Netw. 2008;4(3):15.
[25] Mansour I, Chalhoub G, Lafourcade P. Key management in wireless sensor networks. J Sens Actuator Netw. 2015;4:251–273.
[26] George N, Parani TK. Detection of node clones in wireless sensor network using detection protocols. Int J Eng Trends Technol. 2014;8(6):286.
[27] Ren K, Lou W, Zeng K, et al. On broadcast authentication in wireless sensor networks. IEEE Trans Wireless Commun. 2007;6(7):4136–4144.
[28] Pietro DR, Guarino S, Verde NV, et al. Security in wireless ad-hoc networks – a survey. J Comput Commun. Elsevier. 2014;51:1–20.
[29] Zhang W, Subramanian N. Lightweight and compromise-resilient message authentication in sensor networks. In: Proccedings of IEEE INFOCOM – The 27th Conference on Computer Communications; Phoenix, AZ, USA; 2008. p. 1418–1426.
[30] Wang C, Daneshmand M, Li B, et al. A survey of transport protocols for wireless sensor networks. IEEE Netw J. 2006;20(3):34–40.
[31] Chen CM, Hsu SC, Lai GH. Defense denial-of service attacks on IPv6 wireless sensor networks. Adv Intell Syst Comput. 2015;387:319–326.
[32] Anand M, Ives ZG, Lee I. Quantifying eavesdropping vulnerability in sensor networks. In: Proceedings of the 2nd International Workshop on Data management for Sensor Networks; ACM: Trondheim, Norway; 2005. p. 3–9.
[33] NIST. Skipjack and KEA algorithm specifications [Online]. Available from: http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf
[34] Kumar G, Rai M, Lee G. Implementation of cipher block chaining in wireless sensor networks for security enhancement. Int J Secur Appl. 2012;6(1):57–72.
[35] Zhang Q, Yu T, Ning P. A framework for identifying compromised nodes in wireless sensor networks. ACM Trans Inf Syst Secur. 2008;11(3). 37 p.
[36] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. Security and Privacy, 2003. Proceedings. 2003 Symposium on IEEE. 2003. p. 197–213.
[37] Du W, Deng J, Han YS, et al. A key pre-distribution scheme for sensor networks using deployment knowledge. IEEE Trans Dependable Secure Comput. 2006;3(1):62–77.
[38] Seo S-H, Won J, Sultana S, et al. Effective key management in dynamic wireless sensor networks. IEEE Trans Inf Forensics Secur. 2015;10(2):371–383.
[39] Rizk R, Alkady Y. Two-phase hybrid cryptography algorithm for wireless sensor networks. J Electr Syst Inf Technol. 2015;2(3):296–313.