International Journal of Computing Science and Information Technology, 2013, Vol.1 Iss.03, 10-17
ISSN: 2278-9669, July 2013 (http://ijcsit.org)

Security in Wireless Sensor Network

Yazeed ALKHURAYYIF
Computer Science & Info System. Dept., Shaqra University, Al Quwayiyah, Saudi Arabia.
yalkhurayyif@su.edu.sa

Abstract

Although using wireless sensor networks (WSNs) has been gradually increasing for a number of years now, the design of wireless sensor networks has been criticised as the security issue has not been considered top priority; even though one of the purposes of designing networks is to gather sensitive data. This paper examines and evaluates the current levels of security in WSNs and addresses the WSN's threats, potential attack liability, defined security requirements for WSN, analyses how TinySec and MiniSec meet the requirements. The findings from this paper provide evidence that wireless sensor networks face a number of challenging and ultimately continuing issues due to the lack of priority being given to developing effective solutions.

Keywords: Wireless sensor network (WSN), TinySec, MiniSec, Security

1. Introduction

A wireless sensor network (WSN) is a modern form of technologically advanced computer network. A WSN is a small device containing a processor, light sensors, user and reset buttons, light-emitting diodes (LEDs), a USB interface and 2xAA battery holder. Being a self-configuring network, this means supporting infrastructure is not required when deployed in certain contexts [1]. Sensor modes are used by the medical and military fields to measure constantly varying data from patients and the battlefield environment. Applications include numerous challenging scenarios; including for example, the medical domain where this technology is used to monitor a patient's condition, the military domain to monitor battlefield events and in the public domain to monitor environmental data related to weather or other useful statistics. The WSN is constructed of at least hundreds and up to thousands of nodes, where each node can be connected to one or many sensors.

Due to WSNs' particular characteristics of node mobility, restricted power, limited operating memory and storage space, the task of providing secure communication is more problematic than in traditional networks. Secure link layers should provide for the majority of the security criteria including confidentiality, integrity, data freshness, availability, authentication, authorisation, non-repudiation, scalability, semantic security, and ease of use, in order to ensure a wireless sensor network is secure. The design of WSNs has been criticised as the security issue has not been considered a priority, even though one of the purpose of network design is to collect sensitive data. However, a number of scientists have attempted to prevent the wireless sensor networks' vulnerabilities by introducing numerous security protocols such as TinySec, MiniSec amongst others.

Since their original design and creation, wireless sensor networks have faced a verity of threats and attacks, which may cause disruption to the WSN's functionalities, degrade the WSN performance, destroy partial or whole sections of, to denial of WSN's services, affect the radio frequencies, or disrupt the whole network. However, there are a number of defence mechanisms for detecting and preventing masquerade attacks.

2. Threats and Attacks

2.1. Threats

Wireless sensor networks are more prone to threats than traditional wireless networks because of their inherent characteristics, and may fail to counter internal and external attacks due to their node mobility, restricted power, limited operating memory and other storage space. In addition, WSN nodes can be accessed physically because they are required to be situated near to the working environment. Moreover, WSN nodes are normally tamper-evident as a consequence of cost constraints.

Threats to WSNs can be categorised as follows: [2], [3]:

- **Mote and laptop class attacks:** The mote class attack is only able to access a few sensor nodes; whereas, the laptop class attack is able to access many sensor nodes or even gain complete access to more powerful machines such as a laptop, making the

latter far more harmful.

- **Outsider and insider attacks:** Outsider attacks do not attack nodes that coexist with a wireless sensor network, meaning that an adversary does not become a part of the sensor network. Insider attacks may occur when the key data and code from legitimate nodes are stolen by an attacker who employs a laptop-class machine(s) for the purpose of attacking the sensor network. The insider attacks can also occur when a network user adversely exploits their authorisation. Unfortunately in these cases, the insider attacks are more difficult to detect.

2.2. Attacks and Prevention

Wireless sensor networks are vulnerable to several types of attacks due to their particular characteristics. Protocol stacks which are used by sensor nodes suffer from a multitude of attack methods. These stacks are comprised of layers, physical layer, link/MAC layer, network layer, transport layer and application layer, and all are vulnerable to a range of WSN attacks [4].

Attacks on WSNs can be categorised as either non-invasive or invasive [5]. In general, non-invasive attacks consist of side channel attacks, such as power, timing, or frequency based attacks. However, there is little information on non-invasive attacks whereas invasive attacks have been discussed in many papers. The most commonly occurring attacks on WSNs are called denial of service attacks, which are invasive. DoS attacks on wireless sensor networks can range from a simply jamming communication channels, to sophisticated subversive or even destructive assaults occurring within the protocol's stack layers.

- **Physical layer:** This layer can be exploited by jamming or node tampering attacks. Jamming attacks are the more commonly acknowledged as they occur in wireless communications, and affect radio frequencies or even disrupt whole networks. Tampering attacks physically target WSN nodes and may cause damage to a sensor network or allow unauthorised access to higher levels of communication [6].
  To counter these threats there are a number of defensive methods available. JAM (Jammed-Area Mapping service) is a defence against jamming attacks [7], [8] which can identify any jammed or damaged regions in the sensor network, and instigate measures to protect and restore affected regions. Camouflaging or concealing nodes is a common defence against node tampering attack [6].
- **Link/MAC layer:** According to [9], [6] collision, unfairness and interrogation are all types of the link or medium access control (MAC) layer's attacks. A collision attack occurs during a transmission period in order to disrupt sensor node packets. Unfairness attacks occur when a cooperative MAC layer is abused, leading a node using a real time MAC protocol to fail to meet their deadline. The two-way request-to-send/clear-to send (RTS/CTS) handshake can be exploited by an interrogation attack. A number of MAC protocols employ RTS/CTS handshake to reduce the hidden-node issue. This attack can occur when an adversary sends a myriad of needless RTS messages thereby depleting a node's resources.
  Error-Correcting Codes (ECCs) are an effective protection against collision attacks but its high energy consumption is a major disadvantage. Unfairness attacks can also be prevented by a method called small frames. The aim of this defensive method is to briefly force a single node to capture the channel. Interrogation attacks can be lessened by employing strong MAC layer authentication and anti-replay protection. [9], [6].
- **Network layer:** Hello floods, which overwhelm WSNs by instigating a substantial volume of system responses then disconnecting prior to being completely answered, are the primary network layer attack against WSNs. An adversary using hello floods uses routing protocols to instruct nodes to broadcast themselves as hello messages in order to notify one-hop neighbours of their availability. The attacker then records hello packets and transmits them from a laptop class node with greater transmission capability. The replayed packets will subsequently arrive at nodes unable to directly communicate with the originating node; hence, a node only employing the originating node as the next hop but which lies beyond the node radio range is unable to securely forward traffic. Homing is another form of attack that network layers suffer from. This attack aims to attack any nodes that provide important services, such as monitoring access points or cryptographic key managers, to the networks by using traffic pattern analysis.
  The hello floods attacks can be prevented by pairwise authentication. This method allows any node to verify bidirectional links before constructing routes. Homing attacks can be countered using header encryption. This method's technique is to identify the cluster-head nodes' or base stations' locations by analysing the amount of traffic in different network regions. Unfortunately, this method does not guarantee the security of all traffic analysis. [9]
- **Transport layer:** Flooding attacks occur in the transport layer which manages end-to-end connections. The purpose of this attack is to exploit any protocol that maintains connection information at either end. An example of this can be seen in a TCP SYN flood attack when an attacker first sends a large number of connection establishment requests to the intended protocol, then continues to send connection requests but

never completes the connection. This consumes a WSNs infrastructure and leads to resource depletion. Another transport layer attack is de-synchronisation attack which transmits illegitimate control flags or fake sequence number messages to disrupt an existing connection between two nodes.

SYN cookies are used to prevent flooding attacks by encoding information from the client's TCP SYN message, then directing it back to the client's server to disrupt connection information. Unfortunately, this complicated approach is not desirable for wireless sensor networks. The most appropriate solution to de-synchronisation attacks is to authenticate all packets [9], [6].

- **The application layer:** This layer is vulnerable to attacks called an overwhelming sensors attack. This may lead the network to transmit considerable levels of traffic to a base station allowing an intruder to overwhelm network nodes with sensor stimuli consuming considerable energy and network bandwidth resources. The application layer is also vulnerable to a path-based DoS attack which creates lakes of legitimate traffic in the network caused by excessive use of resources on the data path to the base station. Other nodes in the network are thus unable to send data to the base station. The overwhelming sensors attack can be combated with data-aggregation algorithms. Path-based DoS attacks can be prevented by using both anti-replay protection and packet authentication [9].

As can be seen in **table 1**, wireless sensor networks are vulnerable and therefore subject to a variety verity of DoS attacks. These could create numerous concerns especially if WSNs were used to track sensitive targets in a military scenario, monitor critical production data in an industrial setting or control traffic in a civilian role.

Protocol Layer	Attacks	Defence
Physical	Jamming	Jammed-Area Mapping service
	Tampering	Camouflaging or hiding nodes
Link/ MAC	Collision	Error-Correcting Codes
	Unfairness	Small frames
	Interrogation	Anti-replay protection and authentication
Network	Hello floods	Pairwise authentication
	Homing	Header encryption
Transport	Flooding	SYN cookies
	De-synchronisation	Authenticate all packets
Application	Overwhelming sensors	Data-aggregation algorithms
	Path-based DoS	Anti-replay protection and authentication

Table 1. Denial of service attacks and defence in terms of protocol layers

3. Security Criteria

In order to ascertain whether a wireless sensor network is secure or not, it security requirements need to be precisely determined. The WSN security requirements can be classified as follows: [10], [11], [12], [1]

- **Confidentiality:** this criterion in WSNs means preventing information from unauthorised disclosure that is shared among the sensor nodes or between the sensors and base station. This property is a part of the three key security objectives known as the CIA triad; Confidentiality, Integrity and Availability.
- **Integrity:** the role of data integrity is to guarantee that data has avoided malicious subversion, and consequently remains unchanged, unmodified and intact during the transit period.
- **Data freshness:** this is important to ensure the message freshness is retained even if confidentiality and integrity criteria are provided. It is essential that a secure link layer certifies the freshness of each message. Freshness is either classed as strong or weak.
- **Availability:** to ensure that network services are accessible and usable at any time when required by authorised parties.
- **Authentication:** to ensure that communications in WSN are genuine and that all participants in communications are valid. This principle is required in each base station and sensor node, and authentication properties are also required to establish that the data obtained is actually from both a legitimate source and sender.
- **Authorisation:** to ensure sensors providing information to networks services are authorised and protecting the plaintext from disclosure by unauthorised parties.
- **Non-repudiation:** to ensure that a node is unable to send a previously sent message.
- **Scalability:** inserting or deleting nodes should neither affect the functionality of the security scheme nor increase energy or memory usage.
- **Semantic security:** a state that prevents a monitoring threat from obtaining plaintext or message recovery information, and achieved by ciphering the exact plain-text twice to produce different cipher-texts.
- **Ease of use:** evaluate whether or not a link-layer security protocol is simple, convenient and easy to deploy.

These above security requirements are possibly the most obvious demands for any wireless sensor network.

4. Security Protocols

As wireless sensor networks become popular and extensively employed in numerous fields, a number of interested researchers in the WSN security field have implemented various security protocols in sensor networks.

TinySec and MiniSec are examples of such security protocols.

4.1. TinySec

TinySec is an existing secure network link layer protocol which was developed in 2003. According to its authors, [13] it was the first to establish security link layer for WSNs in particular. This secure link layer was designed to be a lightweight, and amalgamated with TinyOS and thus be easily integrated into sensor network applications. TinyOS is a unique open-source operating system designed for ultra-low-power wireless sensors.

TinySec was specifically designed according to the limited memory and energy capacities and restricted processing capability found in a WSN. The design of TinySec is able to provide two different security possibilities: authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth), which is the default mode of operation. In authentication encryption mode, TinySec encrypts the data payload and also authenticates the packet with a cryptographically resilient message authentication code (MAC). With authentication only mode, the data payload in the TinyOS packet is unencrypted with each entire packet being enhanced with a MAC

TinySec guarantees four of the security criteria: confidentiality, integrity, authentication and ease of use.

- **Message confidentiality:** confidentiality, as described earlier, is defined as preventing secret information from disclosure to undesirable parties. This is can be achieved by encryption techniques such as cipher block chaining (CBC). [13]
- **Message Integrity:** unwanted interference which modifies a message from a legitimate sender during message translation which ought to be detected by the receiver, and employs a MAC for this purpose.
- **Authentication:** for the purpose of ensuring WSN communications are genuine, TinySec employs a block cipher algorithm for encryption. Moreover, for TinySec packets' authentication, a cipher block chaining-message authentication code (CBC-MAC) mode is used.

  Furthermore, MAC is used in TinySec to test message authenticity. [13]
- **Ease of use:** TinySec has been designed as a link-layer security protocol to be easily transparent to applications working with TinyOS. Hence, enablement of this security protocol is common with around 35,000 downloads per year according to the TinyOS homepage.

However, TinySec failed to provide for four important security criteria: data freshness, availability, non-reputation, and semantic security.

- **Data freshness:** unfortunately, neither strong freshness nor weak freshness is provided by TinySec meaning it does not possess the critical capabilities which can prevent many types of WSN attacks.
- **Availability:** TinySec does not guarantee the availability of wireless sensor nodes.
- **Non-repudiation (Replay attack):** TinySec is vulnerable to replay attack which is related to the communication between two parties (a sender and a receiver). An intruder can take advantage if a recipient maintains a limited state level. An intruder, having successfully eavesdropped, replays a legitimate message sent between authorised nodes later. The oblivious receiver consequently accepts the fraudulent message it believes was generated by a trusted sender.
- **Semantic security:** TinySec does not offer semantic security which can prevent an attacker from eavesdropping on plaintext to obtain information. However this lack of semantic security does mean TinySec conserves power - reducing numerous bytes per packet by not sending an individual explicit Initial Values [14].
- **Authorisation and Scalability:** information was unavailable about whether TinySec provides authorisation and scalability or not. However TinySec does not provide the access control service which guarantees resources will be secure [15]. It is therefore unlikely that TinySec possesses authorisation.

4.2. MiniSec

MiniSec is another secure network layer developed after TinySec. Reports indicate that this secure link layer provides higher level of security and lower levels of energy consumption. Other benefits include open source access for developers and users, and simple porting to other platforms. MiniSec operates in two modes, one tailored for single-source communication, or unicast mode, called MiniSec-U, and another tailored for multi-source, or broadcast mode, called MiniSec-B [16], [17].

MiniSec provides for seven of the security criteria: confidentiality, integrity, data freshness, authentication, non-reputation, semantic security and ease of use [5].

- **Confidentiality and Integrity:** both MiniSec-B and MiniSec-U modes possess confidentiality and integrity. For ensuring the confidentiality of data, MiniSec employs offset codebook (OCB) encryption.

  To clarify the progress of investigating whether a message has integrity, two steps are performed. First, OCB encryption using a plain-text message as PM is utilised, then an optimal message header as MH and the nonce as N is used. The plain-text message will be protected with the encryption key (K). The eventual result of OCB $_K$ (N, PM, MH) is a cipher-text {N, PM}

then *K* and a tag of length τ. The message receiver will compute the tag τ to verify message integrity [18], [16].

- **Data freshness:** MiniSec has the desired security property of data freshness. Freshness mostly manages replay attacks. Counter values are used in order for MiniSec to provide weak freshness. In MiniSec-B, each packet has the counter value which can be viewed as plaintext. Whereas in MiniSec-U, through verification of OCB decryption validity, the counter value used for each packet can still be obtained by the receiver. In both modes, the receiver is able to use the counter value mechanism of two messages to enforce message ordering, hence providing reduced weak freshness [16].
- **Authentication:** MiniSec ensures that the communications in WSN is legitimate by using offset codebook mode. The OCB encryption is a block-cipher mode of operation which is able to provide authenticated encryption with just one pass across the message data. [5].
- **Non-repudiation (Replay attack):** MiniSec offers message replay protection in both its modes. With MiniSec-U mode, a synchronised counter is retained by sender and a receiver parties; this counter is employed as the nonce in offset codebook encryption. A replayed packet will be rejected as a receiver would not admit messages unless they possess higher counter values than those maintained in the node state. MiniSec-B prevents replay attacks by dividing the lifetime of the entire network into segments called epochs; MiniSec-B employs loose time synchronization to counter this security obstacle.
- **Semantic security:** MiniSec provides for this by using shared counters instead of random data or initial vectors. MiniSec combines the last x bits of the shared counter with every packet in a message, and is known as Last Bits (LB) optimization. Shared counters emphasize the ordering of messages because a node in a sensor network can verify if a message has been replayed or is out-of order and thus ignore [18].
- **Ease of use:** The MiniSec's source code is both platform independent and publicly available for Telos [1] motes [17].
- **Scalability:** Unfortunately, MiniSec suffers from similar problems regarding scalability as seen in a unicast setup; inserting or deleting nodes may affect the functionality of the security scheme.
- **Availability and Authorisation:** No information is available about this security criterion.

[1] The Telos mote is one belonging to an ultra-low power wireless sensor module.

5. Comparison of TinySec & MiniSec

This part mainly focuses on introducing the similarity and differences between the two security link layers, TinySec and MiniSec, and details their strengths and weaknesses.

5.1. Similarity

MiniSec and TinySec were implemented to provide security for wireless sensor networks, although both do not facilitate key distribution. To compensate for this however, MiniSec uses Localised Encryption and Authentication Protocol (LEAP) for key distribution, while TinySec uses multiple space random key pre-distribution schemes. Both source codes publicly available and have numerous mutual packet format fields such as length (Len), frame control field (FCF), active message (AM), encryption data (Enc Dat) and message integrity code (MIC), as shown in **figure 1** [16], [13], [19].

Len [2][1]	FCF [2]	DSN [1]	DstPAN [2]	DstAddr [2]	AM [1]	SrcAddr [2]	Ctr [2]	Enc Dat [0…29]	MIC [4]

TinySec-AE

Len [1]	FCF [2]	AM [1]	EncDat [0…29]	MC [4]

TinySec-Aut

Len [1]	FCF [2]	DSN [1]	DstPAN [2]	DstAddr [2]	AM [1]	SrcAddr [2]	Enc Dat [0…29]	MIC [4]

MiniSec-U

Len [1]	FCF [2]	DSN [1]	DstPAN [2]	DstAddr [2]	AM [1]	SrcAddr [2]	Enc Dat [0…29]	MIC [4]

MiniSec-B

Figure 1. TinySec packet format (authenticated encryption and authentication only modes) and MiniSec packet format (unicast and broadcast modes).

5.2. Differences

Contrastingly, there are a number of dissimilar aspects between MiniSec and TinySec.

- MiniSec utilises an OCB mode which is a type of block cipher implementation. The OCB mode is able to provide authenticated encryption and secrecy with just one pass over the message data. In contrast, TinySec employs a CBC mode, and require two passes for guaranteed authentication and secrecy. [5]
- TinySec functions only in version one of TinyOS on an older device called the MICA2 mote which is out of production and thus a major limitation compared to

[2] Note all fields are indicated in bytes.

MiniSec's motes, which are operable on current platforms such as the Telos mote.

- TinySec and MiniSec are available on specific mote platforms and considerably unlike. Consequently, it is difficult to confirm the claim of MiniSec's authors that MiniSec only consumes one third the amount of energy of TinySec [16].
- MiniSec provides security mechanisms against replay attack, whereas, TinySec does not.
- MiniSec provides a mechanism in order to guarantee weak freshness, whilst, TinySec lacks this feature. As mentioned earlier, freshness helps to counter many forms of replay attack.
- MiniSec, unlike TinySec, possesses semantic security property.
- In TinySec, whenever two different packets are encrypted with the same initialization vector (IV), there is a high percentage of plaintext recovery [13]. Furthermore, if a message is less than eight bytes then the message cannot be addressed properly. In this situation, the message would be expanded using chipper-text encryption requiring a higher communication cost for sending variable length messages [1]. These issues are avoided in MiniSec as OCB encryption prohibits plaintext retrieval and considers the cipher-text expansion issue by assigning equal length to both cipher and plain text [16].
- TinySec provides two types of mode, including authentication only (TinySec-Auth) mode. On the other hand, MiniSec does not provide a mode without encryption. According to its authors, MiniSec does not support authentication only mode [20], so is unsuitable for socio-environment WSN applications.
- **Table 2** [16] illustrates the comparison between the two secure link layers. TinySec and MiniSec are equal in application data or payload, whilst different in other aspects. The packet overhead, security overhead and total size in MiniSec is two bytes less than in TinySec. This is because MiniSec uses OCB encryption rather than the CBC encryption used in TinySec. MiniSec also employs a synchronised counter when communicating between sender and receiver rather than two passes.

Table 2 also shows that expected energy consumption varies between the two secure link layers; moreover, both MiniSec's variations differ from each other. In normal circumstances, TinySec consumes more than two-thirds the energy of MiniSec making the latter obviously more efficient unless MiniSec-U's packet drop rate rises above 0.9 which rarely occurs (see **figure 2**). Despite the energy issue, MiniSec-B's performance is constant and hence outperforms TinySec. To summarise, MiniSec is far superior to TinySec in every aspects except for those highlighted by other authors claiming the opposite in [21],[22].

	Payload (B)	Packet Overhead (B)	Security Overhead (B)	Total size (B)	Energy Consumption (mAs)
TinySec	24	17	5	41	0.009
MiniSec	24	15	3	39	MiniSec-B 0.004
					MiniSec-U 0.003or more

Table 2. Comparison between TinySec & MiniSec

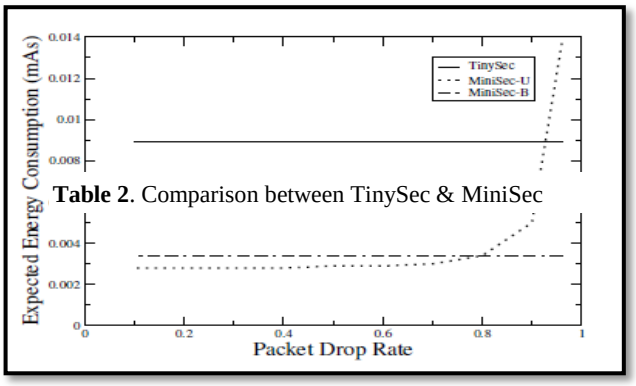

Figure 2. Drop rate [16]

6. Conclusion

Investigating the security aspects of wireless sensor networks has been a challenging and interesting topic. This paper has investigated a variety of threats to wireless sensor network, potential attacks routes, a number of defence mechanisms, WSNs' security criteria, two security link layers known as TinySec and MiniSec and identified the security criteria they possess(outlined in **figure 3 & figure 4**). In addition, this paper has explained the similarities and differences between TinySec and MiniSec (outlined in **figure 5 & table 3**).

It has been therefore proven that wireless sensor networks suffer from numerous threats and attacks as a consequence of the insubstantial designing of the crucial elements of WSNs and apparent ignorance of security issues. TinySec; which is an open-source operating system and the first to actually create a security link layer for WSNs, is rarely used since the release of TinyOS 2.x. As this paper has covered two secure link layers, MiniSec would be the most appropriate security protocol for any wireless sensor networks.

It has become clear from the research into TinySec and MiniSec that both these secure link layers unfortunately failed to provide for all the required security criteria needed for WSNs to be completely secure. It can be safely stated that security is one of the primary challenges to the wireless sensor network entity, and requires serious consideration in order to implement the complete

protocol which would delivers all the crucial security criteria for wireless sensor networks. Until achieved, it is questionable whether sensitive fields, such as the military, should conduct operations using wireless sensor networks, and increased effort is evidently required if these systems are to be fully secure and totally reliable.

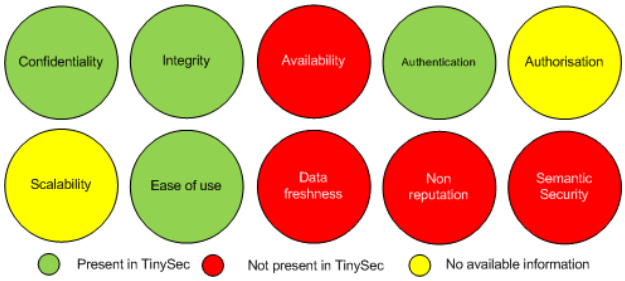

Figure 3. TinySec's security features

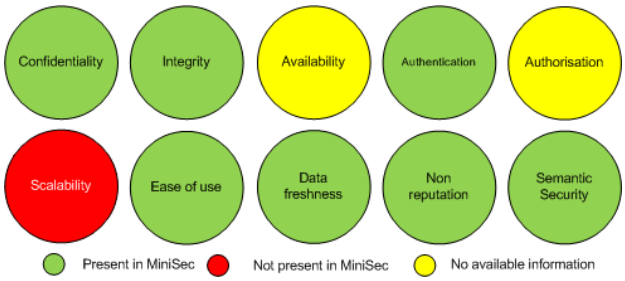

Figure 4. MiniSec's security features

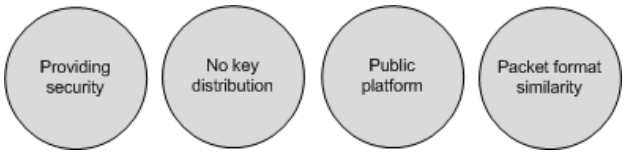

Figure 5. The similarity between TinySec and MiniSec

	Encryption	Secrecy & Authenticity Provision	Platform	Device	Replay Attack Protection
TinySec	CBC	Two passes	TinyOS	MICA2	No
MiniSec	OCB	One pass	Telos	Telos	Yes
	Data Freshness	Semantic Security	Cipher-text Expansion Issue	Recover Plaintet Issue	Socio-environmt Applicability
TinySec	No	No	Yes	Yes	Yes
MiniSec	Weak freshness	Yes	No	No	No

Table 3. TinySec and MiniSec differences

REFERENCES

[1] López, J. and J. Zhou, *Wireless sensor network security*. 2008, Amsterdam; Washington, D.C.: IOS Press.

[2] Tahir, H. and S. Shah. *Wireless sensor networks - a security perspective*. in *Multitopic Conference, 2008. INMIC 2008. IEEE International*. 2008.

[3] Karlof, C. and D. Wagner. *Secure routing in wireless sensor networks: attacks and countermeasures*. in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*. 2003.

[4] Akyildiz, I.F., et al., *Wireless sensor networks: a survey*. Computer Networks, 2002. **38**(4): p. 393-422.

[5] Healy, M., T. Newe, and E. Lewis. *Security for wireless sensor networks: A review*. in *Sensors Applications Symposium, 2009. SAS 2009. IEEE*. 2009.

[6] Wood, A.D. and J.A. Stankovic, *Denial of service in sensor networks*. Computer, 2002. **35**(10): p. 54-62.

[7] Pathan, A.S.K., L. Hyung-Woo, and H. Choong Seon. *Security in wireless sensor networks: issues and challenges*. in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*. 2006.

[8] Wood, A.D., J.A. Stankovic, and S.H. Son. *JAM: a jammed-area mapping service for sensor networks*. in *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*. 2003.

[9] Raymond, D.R. and S.F. Midkiff, *Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses*. Pervasive Computing, IEEE, 2008. **7**(1): p. 74-81.

[10] Mohanty, P., et al., *Security issues in wireless sensor network data gathering protocols: a survey*. Theoretical and Applied Information Technology 2010. **13**(1): p. 14-27.

[11] Madhav, K.V., Rajendra.C, and R.L. Selvaraj, *A study of security challenges in wireless sensor networks*. Theoretical and Applied Information Technology, 2010. **20**(1): p. 39-44.

[12] Sharma, R., Y. Chaba, and Y. Singh, *Analysis of security protocols in wireless sensor network* International Journal of Advanced Networking and Applications, 2010. **2**(3): p. 707-713.

[13] Karlof, C., N. Sastry, and D. Wagner. *TinySec: A link layer security architecture for wireless sensor networks*. 2004. Baltimore, MD.

[14] Karlof, C., et al. *TinySec : TinyOS Link Layer Security Proposal* - version 1.0. 2002 7th July 2011]; Available from: http://cs.uccs.edu/~cs526/studentproj/projF2003/pdcook/doc/design-doc.pdf.

[15] Shaikh, R.A., et al. *Securing Distributed Wireless Sensor Networks: Issues and Guidelines*. in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*. 2006.

[16] Luk, M., et al. *MiniSec: A Secure Sensor Network Communication Architecture*. in *Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on*. 2007.

[17] De Benedictis, A., A. Gaglione, and N. Mazzocca. *Securing a tiered re-taskable sensing system*. in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*. 2010.

[18] Tobarra, L., et al. *Analysis of security protocol MiniSec for Wireless Sensor Networks*. 2007 15 th August 2011]; Available from: https://www.dsi.uclm.es/personal/diegocazorla/pub/41-cibsi07.pdf.

[19] Boujelben, M., H. Youssef, and M. Abid. *An Efficient Scheme for Key Pre-distribution in Wireless Sensor Networks*. in *Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing*. 2008.

[20] Jinwala, D.C., D.R. Patel, and K.S. Dasgupta, *Configurable link layer security architecture for Wireless Sensor Networks.* World Congress on Engineering 2008, Vols I-Ii, 2008. **1**: p. 776-780.

[21] Zia, T., A. Zomaya, and N. Ababneh. *Evaluation of Overheads in Security Mechanisms in Wireless Sensor Networks*. in *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*. 2007.

[22] Roosta, T., S. Shieh, and S. Sastry, *Taxonomy of Security Attacks in Sensor Networks and Countermeasures*, in *The First IEEE International Conference on System Integration and Reliability Improvements*. 2006, IEEE International.