VARIOUS ATTACKS AND SECURITY ENHNACEMENT OF WIRELESS SENSOR NETWORKS.

M.Dahiya[1*], A.Sangwan[2]

[1,2]ECE Department, University Institute of Engineering and Technology (U.I.E.T),

MDU, Rohtak, India.

Abstract:- We all are familiar of the security issues being faced in wireless sensor networks due to various attacks present. The wireless sensor network has various types of advantages as well as some disadvantages. To minimize attacks and to increase security fog computing is done using ONE-TIME PADS (OPTS). The securities of data or information is the most challenging task being faced so far and still a problem which is not completely solved but by using some kind of encryption protocol the security can be enhanced. Some of the encryption protocols are c-sec, zigbee and tiny sec. In this research paper the encryption protocol being used is tiny sec. Tiny sec encryption protocol is the first type of software based protocol. There are various disadvantages of these protocols such as overhead with respect to packet size, time and energy. The tiny sec encryption protocol being used in this research paper uses one time pads (OTPs) due to zero packet losses and lesser overhead. The one time pads (OTPs) are generated using random number generator.

Key Words:- wireless sensor network(wsn), fog computing, cloud, otps.

INTRODUCTION

As we all are familiar that there are two types of networks:-

a) WIRED NETWORK
b) WIRELESS NETWORK

By the name it is clear that a wired network is that network which requires some kind of cables or wires for connectivity. But in case of wireless network no such kind of cables or wires are required. The connection is through air medium. Examples of wireless connection/network are Wi-Fi networks WLAN and wireless sensor network.

TYPES OF WIRELESS NETWORK:-

i. WIRELESS LOCAL AREA NETWORKS(WLAN):-
This type of network requires minimum two devices which shares wireless connection. The distance covered in such network is very less but have a great speed due to restricted hotspots.

ii. WIRELESS MATROPOLITIAN AREA NETWORK(WMAN):-
This network interconnects different users with computer or networks in a geographic region of the size of a metropolitan area.The connection used in this network are point-to-point connections. This network is also known as wireless local loop (WLL). WMANs are based on IEEE 802.16 standard.

iii. WIRLESS WIDE AREA NETWORKS(WWAN):-
In this type of network connection internet can be accessed by WWAN access card or laptop. It have high data rate and the range/distance can be boarded as required.

iv. WIRELESS PERSONAL AREA NETWORK(WPAN):-
This type of networks connection is only established for personally access as numbers of users are limited. It provides high speed but less range.

WIRELESS SENSOR NETWORKS (WSNS):-

WSNs are those networks which require a large scale sensing environment. In this networks the information being present in the environment is sensed and then converted into digital form and is passed to the base node.

TYPES OF WIRELESS SENSOR NETWORK:-

a) Homogenous Networks:-
As the word describes "homo" means "same". So, this network has same type of hardware complexity and battery energy. Only single network topology is used.

b) Heterogeneous networks:-
This type of network is completely opposite to that of homogenous network as it uses different topologies and different battery energy. This type of network is complex type of network.

ADVANTAGES OF WIRELESS SENSOR NETWORKS:-

- Flexibility
- VOIP facility (voice over internet protocol)
- Scalability
- Easy setup
- Less expensive

DISADVANTAGES OF WIRLESS SENSOR NETWORKS:-

- Less secure
- Reliability
- Less speed

ATTACK AND ITS TYPES:-

The term attack means any kind of act which leads to disturb the network.

TYPES OF ATTACKS:-

- Sybil Attack:-
  This attack is the vulnerable attack onto the wireless sensor network. The mechanism followed in this attack involves a case node and some other nodes which having different identical legal nodes. By this mechanism it is clear that one single node can be connected to different nodes in the network. The Sybil attack can be prevented by authentication and encryption mechanism.
- Wormhole Attack:-
  The most important attack is this wormhole attack in wireless sensor network. In this attack the attacker saves/stores some of the packets at some particular location and then transmits them at another place. This attack is most risky to wireless sensor network as this attack do not require compromising the sensor in the network or other.
- Denial of Service Attack(DOS):-
  This attack can disturb the transmission side of the wireless sensor network due to which some kind of noise, collision can occur that can disturb receiver side. Some targets such as network access, infrastructure and server application which the attackers used to reach. This attack not only destroys or disturb the network but it also end the capability of the network for not allowing further service in future.
- Hello Flooding Attack:-
  In this attack a packet named as "HELLO" is employed which acts as a weapon in the network to access the sensors present in the network. The attackers who have the highest radio transmission amongst other attackers will further process the power transfer Hello packet to many other nodes which are separated in a wide area network.
- Sinkhole Attack:-
  This attack is the most dangerous attack in which the base station is not able to receive accurate and correct sensing data. The goal of sinkhole attack is to establish a metaphorical sinkhole having adversary at the centre. Sinkhole attack uses routing algorithm by which a particular node attract the neighboring node.

Now a days we all are aware that IOT (INTERNET OF THINGS) has the major role in connecting and communicating with each other over the internet. Now, devices such as microwave ovens, car and many more are connected to internet which was not even thought off in the past. Connecting and communicating over internet has lead to easy access to make decisions regarding anything in any kind of business at a low cost.We know that there is a different variety of data present in environment and these data are constantly being generated and transmitted over the internet. Depending upon the type of devices connected the data may be stored or processed further. The IOTs main characteristic is the cloud as it reduces the replicate different types of software and hardware. The cloud is used to store and process the data.The challenging issue being faced by the IOT is the present cloud representation can not handle the generated data from IOTs. Latency, bandwidth utilization and throughput are some problems fased by IOTs. Solution to these issues/problems is fog computing.Fog computing is a type of model which permits data to process from IOT to the edge of the network without involving cloud. Later the data can be sent to cloud for storing or for further processing.

- Fog computing minimizes the latency and conserve the bandwidth of network.
- The devices known as fog models help in ensuring security and can process different types of data.
- Fog applications allow the fog nodes to receive data and process the data to their optimal places. The data which is time sensitive and cannot be delayed are analyzed by the fog nodes where as the data which have the waiting property are analysed by aggregated nodes.

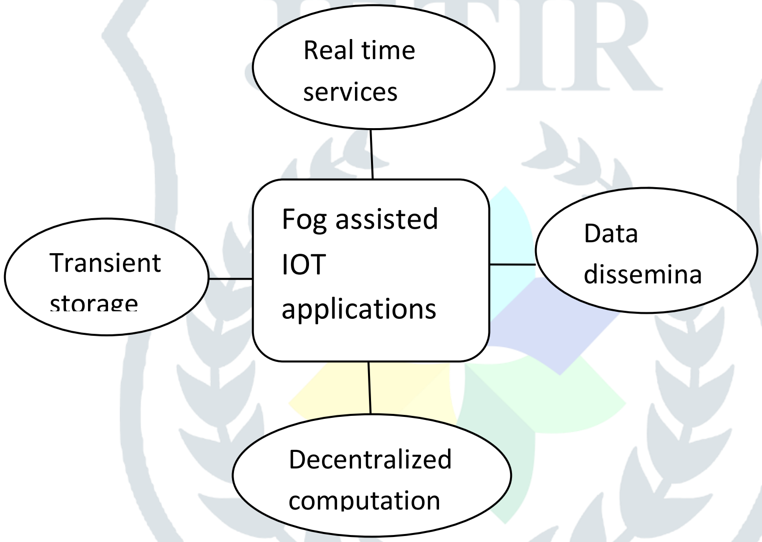

Fig. 1.Fog computing roles [6]

A survey was done by Ni et al.[6],in which was cleared that fog computing has its own security challenges. Accessing the data from the device becomes difficult for the attackers as analyzing and storing the data in fog nodes is done locally by which the dependence on internet connectivity is decreased. It is also seen that the exchange of data from sender to the receiver is not in real-time so it was difficult for the attacker to constantly anticipate or except whether to interrupt the data. Fog computing have some security enhancement but still it has its own drawback in the field of privacy and security. There are many threads regarding security and privacy and they can be minimized by using various protocol which are not being discussed in this paper. This paper helps in reducing latency and energy overhead in comparison to other protocols by using one time pads (otp). In 1917, the OTP was introduced as encryption scheme having high security. This is a encryption scheme in which the length is equal to the length of plain text and is used only Once. Modular addition (XOR) of the plain text and key generates the cipher text and is difficult to decipher it. This research generates the OTP by using RNG(random number generator).

RELATED WORK

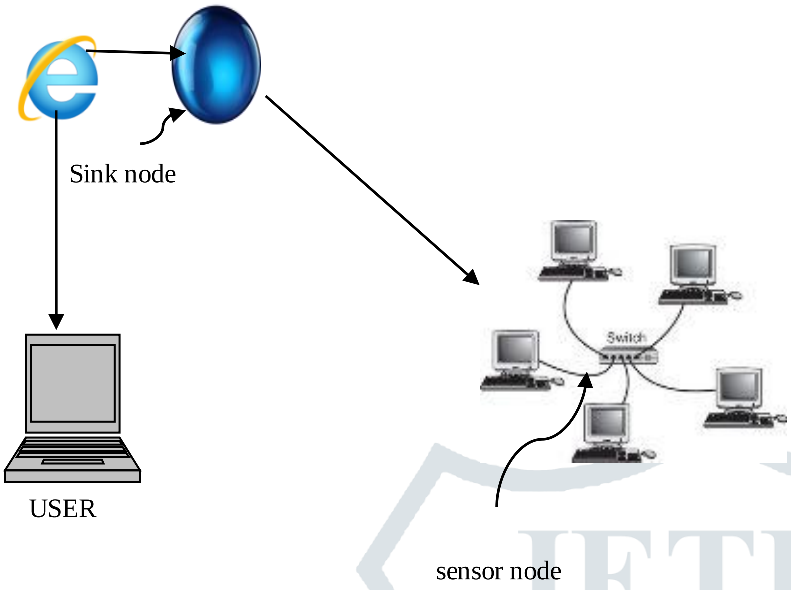

Fig no. 2. Wireless Sensor Network

A term named as Sensor nodes or motes which can feel, operate and further dispatch the information which is attained from the nature to the station via radio are resource constrained devices present in Wireless sensor networks. These are placed in spaces which can be approached and unapproached by human beings. According to their characteristics these applications have many applications as in military, environment and health.The highest place of strain in energy conservation of mote is radio communication. As the consumption of energy at the reception side is twice of then processing in Micaz (14) Mote, radio usage is minimum.To ensure that the working of motes is efficient for a long period there are challenges (15) like security, routing, clustering and data aggregation.Physical comprise of modes, management, distribution of keys and data security are the challenges being faced in security issue.The protocol being used generates overheads related to packet size, energy, time satisfies the data security issues. Various surveys have been done to determine which kind of encryption algorithms would be best for encryption protocols.AES (Advanced Encryption Standards) is the most efficient algorithm.

This paper ensures great data security and 0% packet overhead and also low energy, time overheads in comparison to other protocols by using one time pads based encryption protocols. The research done by Boakye-Boateng et al.(22) is being further researched in this paper which successfully encrypt and decrypt by XORing packets with one key in a single effort to attain possible use of OTPs in tiny OS(Tiny Operating Systems).There are various types of encryption protocols such as Secure Network and Encryption Protocol (SNEP), Mini Sec (25), Zigbee (23), Tiny Sec (26) and C Sec (21). Hardware implemented protocols are Zigbee, SNEP, Mini Sec and C Sec whereas Tiny Sec is software based protocol. Message Authentication Code (MAC) which is a cryptographic checksum of a message is implemented on Tiny Sec, SNEP and Mini Sec for ensuring integrity of data.Tiny Sec and C Sec are further discussed in this paper. These two protocols are selected due to two reasons:-

- As in Tiny OS overhead is a software based protocol.
- C-Sec as mentioned in [Table 1 and Table 2] is the most efficient hardware based protocol.

Research is also done in the field of Body Area Network (BAN's) by [27] using OTP's is also discussed in this paper.

A. Tiny Sec

The first ever software based protocol is Tiny Sec [26].

In this data is encrypted in specific blocks and each block is dependent upon previous block for decryption. This scheme is known as cipher-block chaining (CBC).

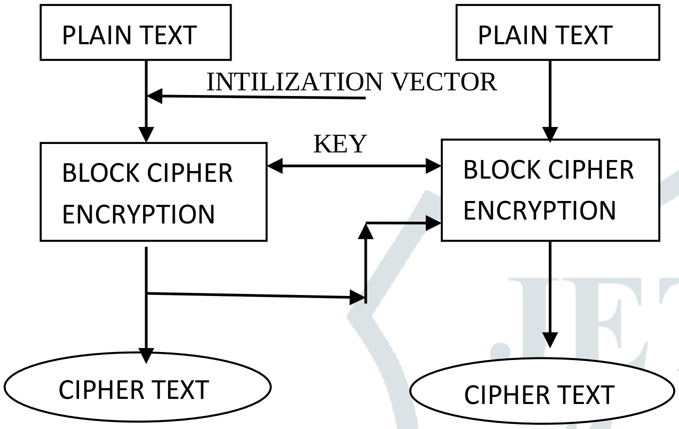

Figure 3 CBC Encryption Scheme.

This scheme contain an Initialization Vector (IV) which ensures that the cipher texts are not similar to plain text. Integrity and authentication are ensured by calculating MAC using CBC.The secret key shared by the receiver and the sender is used for the computation of the MAC. Any packet is received only if the calculate MAC matches to the MAC generated by the sender. Two security options with packet latency of 8% and 1.5% named as Tiny Sec AE (responsible for authentication and encryption) and Tiny Sec Auth (responsible for authentication) respectively.

B.C-SEC[21]

The cipher text is generated by implementing cipher feedback(CFB) encryption scheme using AES encryption algorithm. To ensure data freshness C-SEC protocol is used by communicating nodes. It also ensures the integrity and authentication by implementing HMACs(Hash-Based MACs). Two modes of operation operated by C-SEC protocol is

- CONVENTIONAL MODE(C-Sec$_{cpt}$)
- COMPACT MODE(C-Sec$_{conv}$)

CONVENTIONAL MODE(C-Sec$_{cpt}$):-In this type of mode operation the security information is stored in starting or ending part of the packet.

COMPACT MMODE(C-SEC$_{conv}$):- This mode of operation works when two packets are to be transmitted.

In the conventional mode the sender and the receiver are required to store the HMACs of the end packets.

C.OTP ENCRYPTION ON BANS

An OTP based encryption protocol for Body Area Networks(BANs) which is on software level is implemented by Bushing et al.[27]in which various parameters were compared such as speed, hardware based AES encryption protocols in which the outcomes were favorable. In this scheme the main drawback was the use of SD CARD. As the SD card used to store the information and is being refreshed after every fixed interval of time. Those nodes which do not have SD cards in them were not useful such as MICAz[14] and TelosB[29].

TABLE 3

NOTATION BEING USED

P= transmitted/received packet.

Str=source address of packet “p”.

Dst=destination address of packet “p”.

Dsn=data sequence number of packet “p”.

Fcf=frame control field of packet “p”.

Crc=cyclic redundancy field of packet “p”.

payload =payload field of packet “p”.

lpayload =payload field length.

i=counter used for loop starting from zero

payload [i]= i^{th} byte of a payload.

$\oplus$ = XORing operation.

K=OTP or key to encrypt packet “p”.

Kstr=subset of key, used to encrypt str.

Kdst=subset of key, used to encrypt dst.

Kdsn=subset of key, used to encrypt dsn.

Kcrc=subset of key, used to encrypt crc.

Kpayload=subset of key, used to encrypt payload.

$\leftarrow$ = Assignment operator.

node_id =sensor node identification number.

m =sleep mode/time.

n =new packet arrives.

TABLE 2

COMPUTATION AND COMMUNICATION OVERHEAD OF EXISTING ENCRYPTION PROTOCOL[28]

PRO	TIME OVERHEAD			ENERGY OVERHEAD		
	Comp.	Comm.	Total	Comp.	Comm.	Total
SNEP	240	312.48	552.48	13.44	9.16	22.6
MINI SEC	380	252.45	632.45	9.12	9.068	18.19
TINY SEC	380	249.98	629.98	9.12	7.32	16.44
ZIGBEE	25	374.98	399.97	0.35	10.99	11.34
C-SEC$_{cnv}$	3.82	253.88	257.7	0.207	9.257	9.48
C-SEC$_{cpt}$	3.82	3.9	7.72	0.207	0.115	0.322

Steps to be followed for generating a 2 byte k_{str} key

1. Encryption algorithm

Steps:-

a) In the very first step we will assign str equal to str+k_{str}. (i.e; str = str k_{str})
In this step the k_{str} key is obtained b$\oplus$ the RNG XoRED with the str field to encrypt the field.

b) This step includes generation of 2 byte k_{dst} by assigning k_{dst} equal to dst+k_{dst}.
(i.e; dst $\leftarrow$ dst k_{dst})

In this step the k_{dst} key is obtained b$\oplus$the RNGnXoRED With the dst field to decrypt the field.

c) Now in this step 1 byte k_{dsn} key is generated by assigning dsn equal to dsn+k_{dsn}.
(i.e; dsn $\leftarrow$ dsn $\oplus k_{dsn}$)
In this step the same processing is followed which is used in above two steps.

d) In this step an "I" integer is taken whose counter is starting from ZERO and is assigned in loop as

Loop {For i=0&&i< lpayload do}.loop end

e) Now we will generate 1 byte $k_{payload}$ key by simply assigning payload[i] equal to payload[i]+$k_{payload}$.
(i.e; payload [i] $\leftarrow$ payload[i] $\oplus k_{payload}$).

f) Now generating 2 byte k_{crc} key by the same process that is being used above.(i.e; assigning crc crc k_{crc})

g) Now as the packet (P) is r$\leftarrow$ady to b$\oplus$ansmitted so it is bei$\leftarrow$g transmi$\oplus$ed.

h) Now as the packet is transmitted then for a short period of time say "m" the key is stopped or putted on sleep mood so that replays can be ignored.

i) When a new message or packet arrives let say "n" the key wakes up automatically so that no delay occurs.

2. DECRYPTION ALGO

Steps:-

a) In the very first step we will assign str equal to str+$k_{str.}$

(i.e; str ← str ⊕ $k_{str)}$In this step the k_{str} key is obtained by the RNG XoRED with the str field to encrypt the field.

b) This step includes generation of 2 byte k_{dst} by assigning k_{dst} equal to dst+$k_{dst.}$
(i.e; dst ← dst k_{dst})In this step the k_{dst} key is obtained by the RNG XoRED
With the dst field to d⊕crypt the field.

c) Now in this step 1 by⊕ k_{dsn} key is generated by assigning dsn equal to dsn+k_{dsn}.
(i.e; dsn ← dsn k_{dsn})
In this step the same processing is followed which is used in above two steps.

d) In this step an "I" integ⊕is taken whose counter is starting from ZERO and is assigned in loop as

Loop {for i=0&&i< lpayload do}.loop end

e) Now we will generate 1 byte $k_{payload}$ key by simply assigning payload[i] equal to payload[i] +$k_{payload.}$
(i.e; payload[i] ← payload[i] $k_{payload}$).

f⊕ Now generating 2 byte k_{crc} key by the same process that is being used above.

(i.e; assigning crc ← crc k_{crc})

g) As now the packet is received a⊕d decrypted it is checked if the received message or dst is same as transmitted message str.

h) For this a loop is used which will check is dst is equal to node_id (i.e; sensor node identification number).

i) If the dst is equal to node_id then the packet is accepted.

j) But if dst is not same as node_id then the packet is dropped.

k) In the last an acknowledgement message is send back to the sender to inform that the packet is received correctly or not.

IMPLEMENTATION AND EVALUATION.

It was investigated in the previous research (22) that it is possible to XOR the packets and their energy overhead in Tiny OS using only a single key which helps in creating an OTP protocol. The implementation of this research was done on the Tiny OS application. Where a node leads to broadcast the message contains payload of four byte which stores the sender address and a counter as well. Three LEDs will be turned on according to the last three bits of the counter at receiver side when the receiving node will receive a message. It is expected that the counter value after decryption at receiver side matches to the counter value at the time of encryption at sender side. The energy overhead received was less than 0.1 micro joule. The encryption and decryption of the payload is done on the active message layer where as process of dsn, dst and str is done on the transmit/receive P layer. Implementing was done for two Micaz motes by using Avrona emulator. It was observed that storing the OTPs on Micaz were not energy efficient while investigating the generation of OTPs with in the node it was observed that RNGS (RANDOM NUMBER GENRATORS) was required. Two RNGs were considered in the TinyOS which were

- LFSR(LINEAR FEEDBACK SHIFT REGISTER)RNG
- MLC(MULTIPLICATIVE LINEAR CONGRUENTIAL)RNG

LFSR is a 16-bit RNG where as MLC is a 32-bit RNG. The faster RNG among these two is LFSR RNG. Both the RNGs were ideal as they are designed with resource constraints in focus. Two RNGs were cloned which were from LFSR RNG and similarly two were from MLC RNG. The cloned RNGs were used to perform two different operations. One for encryption and one for decryption process. For dest , src and crc fields a 16 bit RNG value is generated for each of them. For payload field the RNG value generated can be either 16 bit or 32 bits which depends on the lpayload size whether it is of 2 or 4 bytes. Only 16 bit values were generated by the RNG and to decrypt 1- byte dsn field 4 bits are shifted to the right side. Encryption for fcf , length, destpan, type and network is not performed. A failure occurred when the destination and source address were not correctly verified by the receipt node which was due to the two cloned-MLC RNGs being implemented on Tiny OS application which failed to activate the LEDS. The failure occurred at the receiver end at the time of decryption of message as encryption process was performed correctly. Due to MLC RNG the decryption becomes impossible. But this problem which was not seen in case of LFSR RNG as it activates the LEDs to match the counter. But the problem which was being faced by this was that energy readings were more than 8 micro joule. Which was resolved by performing encryption and decryption in the transmit P/receive P layer. The memory address of payload was offset by 2 bytes to get actual payload field which tells about the effectiveness of encryption and decryption of payload. Comparison of different protocol overhead with OTP protocol overhead was shown in the table IV.

TABLE IV

comparison of overhead with OTP protocols.

Protocol	Time overhead	Energy overhead	Packet overhead(%)
OTP	163.5	0.89	0
SNEP	552.48	22.6	27
MiniSec	632.45	18.19	16.60
Tiny sec	629.98	16.44	22
Zigbee	399.97	11.34	32
C-sec $_{cnv}$	257.7	9.48	16.60
C-sec$_{cpt}$	7.72	0.322	-5.40

CONCLUSION

The final conclusion made from this research shows that it is feasible to generate an OTP based encryption protocol for wireless sensor networks (WSNS) with random number generators (RNGS).

It can also be concluded that latency of the network will improve with improvement in fog application and in short the entire for computing will be improved. For ensuring protection against authentication, integrity, confidentiality, replays and many other factors related to security of the protocol have been successfully achieved .

The existing protocols fails when replay action is performed in the network as the key is used only once so it becomes difficult to decrypt the packet leading to unsuccessful description the thus discarding the packets.

This paper had successfully removed the problem of replays as the nodes goes in sleep mode does avoiding the replays of the package for a “m” period but before such action a message is sent to the all the nodes to inform them about such kind of actions.

Due to unsuccessful description on source and destination the authentication fails automatically. The unsuccessful description is because the recipient node would not be aware of the resulting address. The integrity is secured by this protocol as tempering the messages leads to disturb the CRC field which at the time of description do not disclose the actual value of CRC. As the packets are not able to descript and with the evenly distribution nature of OTP the confidentiality is secured/ensured. As the OTPs generated through random number generator they can strength the protocols. It can also be seen the strength of protocol depends upon the type of RNG implemented.

As the LFSR RNG was successfully implemented and worked it have some drawbacks such as the key space is limited. It has been noted the more Complex algorithm of RNG will affect the time and energy overheads. It is considered to have different RNG for encryption and description even though the RNG are identical. The RNG used for encryption should be used for RNG used for description and vice versa.

REFERENECES

[1] M. Chiang and T. Zhang, “Fog and IoT: An overview of research opportunities,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854– 864, 2016.

[2] H. Farhangi, “The path of the smart grid,” IEEE power and energy magazine, vol. 8, no. 1, 2010.

[3] F. Computing, “the internet of things: Extend the cloud to where the things are,” Cisco White Paper, 2015.

[4] B. Hayes, “Cloud computing,” Communications of the ACM, vol. 51, no. 7, pp. 9–11, 2008.

[5] G. Premsankar, M. D. Francesco, and T. Taleb, “Edge Computing for the Internet of Things: A Case Study,” IEEE Internet of Things Journal, vol. PP, no. 99, p. 1, 2018.

[6] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing fog computing for internet of things applications: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8066283/

[7] A. D. Wood and J. A. Stankovic, “A taxonomy for denial of-service attacks in wireless sensor networks,” Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, pp. 739–763, 2004.

[8] X. Lin and X. Li, “Achieving efficient cooperative message authentication in vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3339–3348, 2013.

[9] I. S. Technologies, “European Network of Excellence in Cryptology,” 2002.

[10] B. Schneier, Applied cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2007.

[11] Y. Sharma. (2015) What is wireless sensor network (WSN) technology?[Online]. Available: https://www.quora.com/What-is-wireless-sensornetwork- WSN-technology

[12] B. Wang, X. Gu, L. Ma, and S. Yan, “Temperature Error Correction Based on BP Neural Network in Meteorological Wireless Sensor Network,” International Journal of Sensor Networks, vol. 23, no. 4, pp. 265–278, 2017.

[13] E. Shih, S.-H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, “Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,” in Proceedings of the 7th annual international conference on Mobile computing and networking. ACM, 2001, pp. 272–287.

[14] C. Technology, “Crossbow, MICAz Datasheet and Manual, MIB Mote User,” 2003.

[15] S. B. Othman, A. Trad, and H. Youssef, “Performance evaluation of encryption algorithm for wireless sensor networks,” in Information Technology and e-Services (ICITeS), 2012 International Conference on. IEEE, 2012, pp. 1–8.

[16] M. Almasri, K. Elleithy, A. Bushang, and R. Alshinina, “TERP: A Trusted and Energy Efficient Routing Protocol for Wireless Sensor Networks (WSNs),” in Proceedings of the 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications. IEEE Computer Society, 2013, pp. 207–214.

[17] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, “Efficient and provably secure aggregation of encrypted data in wireless sensor networks,” ACM Transactions on Sensor Networks, vol. 5, no. 3, pp. 1–36, may 2009.

[18] S. Zhu, S. Setia, and S. Jajodia, “Leap+: Efficient security mechanisms for large-scale distributed sensor networks,” ACM Transactions on Sensor Networks (TOSN), vol. 2, no. 4, pp. 500–528, 2006.

[19] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[20] F. Zhang, R. Dojen, and T. Coffey, “Comparative performance and energy consumption analysis of different AES implementations on a wireless sensor network node,” International Journal of Sensor Networks, vol. 10, no. 4, pp. 192–201, 2011.

[21] A. Moh’d, N. Aslam, W. Robertson, and W. Phillips, “C-sec: Energy efficient link layer encryption protocol for wireless sensor networks,” in Consumer Communications and Networking Conference (CCNC), 2012 IEEE. IEEE, 2012, pp. 219–223.

[22] K. Boakye-Boateng, E. Kuada, and E. Antwi-Boasiako, “Efficient encryption protocol for wireless sensor networks using one-time pads,” in Electrotechnical Conference (MELECON), 2016 18th Mediterranean. IEEE, 2016, pp. 1–6.

[23] Z. Alliance and Others, “Zigbee specification,” 2006.

[24] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: Security protocols for sensor networks,” Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[25] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “Minisec: a secure sensor network communication architecture,” in Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on. IEEE, 2007, pp. 479–488.

[26] C. Karlof, N. Sastry, and D. Wagner, “Tinysec: a link layer security architecture for wireless sensor networks,” in Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004, pp. 162–175.

[27] F. B¨usching and L. Wolf, “The rebirth of one-time pads—secure data transmission from ban to sink,” IEEE Internet of Things Journal, vol. 2, no. 1, pp. 63–71, 2015.

[28] S. M. AlMheiri and H. S. AlQamzi, “Data link layer security protocols in wireless sensor networks: A survey,” in Networking, Sensing and

Control (ICNSC), 2013 10th IEEE International Conference on. IEEE, 2013, pp. 312–317.
[29] T. Crossbow, "Telosb data sheet (2010)."
[30] D. Gay and J. Hui, "Tep 103: Permanent data storage."
[31] P. Levis, "TEP 111: message t," Core Working Group, TinyOS Community, 2010.
[32] A. F. Molisch, K. Balakrishnan, D. Cassioli, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster et al., "IEEE 802.15. 4a channel model-final report," IEEE P802, vol. 15, no. 04, p.0662, 2004.
[33] C. C. Datasheet, "2.4 GHz IEEE 802.15. 4," ZigBee-Ready RF Transceiver (Rev. B), 2012.