International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 03 Issue 02 | 2016

Security of Wireless Sensor Networks

Yugandhara L. Rothe

Department of Computer Engineering, Dr VBKolte College of Engineering, Malkapur, Sant Gadge Baba Amravati University

ABSTRACT

Wireless sensor networks have been researched extensively over the past few years. They were first used by the military for surveillance purposes and have since expanded into industrial and civilian uses such as weather, pollution, traffic control and health care. One aspect of wireless sensor networks on which research has been conducted is the security of wireless sensor networks. These networks are vulnerable to hackers who might go into the network with the intent of rendering it useless. An example of this would be an enemy commandeering a drone and getting it to attack friendly forces. In this paper, we review the security of wireless sensor networks. Areas that are covered include: architectures and routing protocols, security issues that include context and design as well as confidentiality, integrity, and authenticity, algorithms, and performance issues for wireless sensor network design. Performance of the Self-Originating Wireless Sensor Network (SOWSN), Practical Algorithm for Data Security (PADS), and mechanisms for in-network processing were investigated in further detail with SOWSN having the best performance as a result of it being based on realistic scenarios.

Keywords: Self-Originating Wireless Sensor Network (SOWSN), Practical Algorithm for Data Security (PADS),and mechanisms for in-network processing were investigated in further detail with SOWSN.

I. INTRODUCTION

A Wireless Sensor Network (WSN) can be defined as a group of independent nodes, communicating wire lessly over limited frequency and bandwidth [1]. The novelty of WSNs in comparison to traditional sensor networks is that they depend on dense deployment and coordination to execute their tasks successfully. This method of distributed sensing allows for closer placement to the phenomena to be achieved, when the exact location of a particular event is unknown, than is possible using a single sensor [2],data security has received little consideration. In order for ubiquitous computing to become a reality, system security and privacy protection need to be assured. Securing data streams in sensor networks is important because traditional encryption and authentication protocols such as Tiny Sec are often unable to keep up with high stream rates, and they deplete the network of energy too quickly [3]. Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN. Information based on sensed data can be used in agriculture and livestock, assisted driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance. Five key features need to be considered when developing WSN solutions: scalability , security, reliability, self-healing and robustness.

Practical Algorithm for Data Security (PADS) method to provide protection against Base Station Sensor Nodes Routing Links Shared Secret passive eavesdropping by employing confidential transmissions of data messages. For each transmission, a one-time pad (OTP) is created. A secret key and the MAC calculated over the data are used to create the OTP. When the OTP is combined with the data, data encryption and data integrity are achieved at the same time.The PADS protocol only adds 4 bytes, making it even more efficient than SNEP. Just as with SNEP, PADS also provides data confidentiality and semantic security. Semantic security implies that eavesdroppers cannot infer the data even if they see the same data encrypted several times. The PADS protocol has dynamic key sizes and the ability to change the number of bytes to be encrypted. By using one-to-one routing and pair-wise shared keys, data integrity is guaranteed. At the worst, the algorithms run in linear time on the size of the reading, regardless of the size of the network. The correctness of the algorithms was proven and the theoretical analysis of the energy usage shows that the application is appropriate for sensor networks. Simulations have shown this protocol to be suitable for sensor networks. where the simulation results are provided. The simulation shows that the overhead due to the algorithm is negligible, and the performance of a network with the protocol is similar to a network without additional security. Compared with a network using encryption and authentication using Tiny Sec, the performance of a network using this study's protocol is much better in terms of throughput, delay and energy consumption per message received at the base station.

II. BACKGROUND

In this study of security for wireless sensor networks, we basically use two methods which is basically work in algorithm as

1.Self-Originating Wireless Sensor Network (SOWSN)
To design a completely secure WSN, security must be integrated into every node of the system. Any component of a network implemented without any security could easily become a point of attack.Resultantly this dictates that security must pervade every aspect of the design of a wireless sensor network application that would collect or disseminate sensitive information; i.e. requiring a high level of security [4]. Conventional networks require protection against eavesdropping, injection or modification of disseminated data packets, and accordingly, most applications of WSNs require the same protection. Cryptography is the standard method of defense against such attacks [4]. This defense brings with it a number of other trade-offs. Varying levels of cryptographic protection implies, proportionately varying level of overhead;in the form of increased packet size, code size, processor usage etc. This is the stem of all debate relating to optimal security techniques in WSN.

2.(PADS)
This algorithm helps in implementatio n of the practical algorithm for data security of PADS an end to end security scheme employing symmetric key encryption.The implementation takes full advantage of the modular design of the tiny Operating System environment.The simplicity of the algorithm allows for efficient implementation in hardware,requirement for resource constrained devices.

III. PREVIOUS WORKDONE

Akyildiz,I.F, Su , W., Sankarasubramaniam, Y. , Cayirci ,E.,[1] works on sensor networks ‘A Survey on Sensor Networks and self originating wireless sensor networks.
M. Acharya, J. Girao, D. Westhoff, [2] based on PADs "Secure Comparison of Encrypted Data in Wireless Sensor Networks also on encryption,data security."
Chee-Yee Chong, and Kumar,S. P,[3] works on“Sensor Networks: Evolution, Opportunities, and Challenges and history of sensor networks”
Wireless sensor networks : “security and architecture” having architecture of tiny OS and its mechanism.
Security in cognitive wireless sensor networks.:-Challengesand open problems woks on challengs in wireless technology and its advantages also on disadvantages.

IV. ANALYSIS AND DISCUSSION

There are some definations steps which are used in Wireless sensor networks Tiny practical protocol of data security as follows
Definition 1:-A message authentication code (MAC) is the result of applying a public function to the input using a secret key. The MAC is of fixed length, is attached to the input and serves to prove integrity and authenticity of the input. A MAC is also known as cryptographic checksum [6].
Definition 2:-A MAC function is a function used to generate a MAC. A MAC function has three properties. It is a one-way function, that is, given a MAC it is computationally infeasible to find the original input. It offers weak collision resistance, that is, it is computationally difficult to an a second input (= the first input) which produces the same MAC. It offers strong collision resistance, that is, it is computationally difficult to find two inputs which produce the same MAC[6].
Definition 3:-A CBCMAC function is a function which uses a block cipher in cipher block chaining (CBC) mode to generate MAC codes. A CBCMAC is created by encrypting the input into a chain of blocks, such that each block is dependent on the previous block [6].
Definition 4:-A one-time pad is a sequence of bits that is XOR to the reading in order to provide protection against eavesdropping.
Definition :-5. Ki is the secret master key shared between node i
and the base station. The value of k i can be updated similar to
updating keys in [7] and [8].
Definition 6. kij is the jth secret key shared between node i and the base station. The key is periodically updated to guarantee freshness.
Definition 7:-xij is the data value x generated at time j by node
i. xi is the current value of x

Address/msg type	ID	Data length	Source, original address	Sequence number	Hope count	Type byte	Parent aderss (2)byte	MAC bytes(4)	CRC bytes(2)

Figure 1:Multihop packet structure for MAC Calculation

generated by node i and p(xij) is the packet generated by node i at time j, which contains the sensor value x.
Definition 8. b(x) is the bit size of the value x. b(MAC) is the bit size of the Message Authentication Code (MAC).
Definition 9. α determines the length of the subsequence of the MAC. β determines the starting location of the aforementioned subsequence of the MAC. α, β ∈Z.

V. PROPOSED METHOD

Algorithm:-
ALGORITHMS:- The one-time pad is constructed by the nodes using only information contained within the data packet and the secret key shared between the sender and the base station. First, the MAC (message authentication code) is calculated based on the sensor reading. Next, a one-time pad is constructed from the MAC and the key shared with the receiver. The MAC is attached to the sensor reading. The variables α and β are calculated based on the MAC, and a sub-sequence of the MAC is extracted and used to secure the sensor reading. The receiving node uses the attached MAC, removes the encryption, and calculates its own MAC. To show that the message has not been tampered with, the two MACs are compared for equality Algorithm of Embedding of a one-time pad

```
Basic Embedding Algorithm: embed Require: kij , packet p(xi) of sensor value xi Ensure: p(xi) XOR with the one-time pad
1: calculate MAC over p(xi) and save in p(xi) 2: ktime = kij modified and time synced
3: α = ktime mod b(MAC)+1
4: β = ktime mod (b(MAC) − α + 1)
5: temp pad = substring of MAC starting at α for β bits 6:pad = Append temp pad to pad until pad is of the same length as the data
7: xi = xi XOR pad
8: Replace xi with xi in p(xi) and send
```

VI. RESULT AND ANALYSIS

The self originating wireless sensor network and practical algorithm of data security is the correct algorithm for the security purpose of wireless sensor network. The algorithm PADs shows data in sensor networks can be securely routed through the network which wherever we use like MAC, security, encryption etc.

VII. CONCLUSION

In this we study the self originating wireless sensor network using denial of attack and cryptographic mechanism. And also study the practical algorithm of data security(PADs).In this paper studies the algorithm of PADs Using MAC i.e. Message Authentication code base one one time padding algorithm.

VIII. FUTURE WORK

In the security of wireless sensor network there will be lots of variation is coming soon as generation of various wireless sensor network and this technology used in various security purpose. Future work will include applying the one-time pad protocol to data aggregation and data fusion.

IX. REFERENCES

[1]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci,E. (2002) 'A Survey on Sensor Networks', IEEE Communications Magazine, 40(8), 102-114.

[2]. Bharathidasan , A., Anand, V., Ponduru, S. (2001), Sensor Networks: An Overview, Department of Computer Science, University of California, Davis 2001. Technical Report

[3]. C. Karlof, N. Sastry, and D. Wagner. Tiny sec: A link layer security architecture for wireless sensor networks.In Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004), November 2004

[4]. Perrig, A., Stankovic, J., Wagner, D. (2004), “Security in Wireless Sensor Networks”, Communications of the ACM, 47(6), 53-57

[5]. Chee-Yee Chong, and Kumar, S. P. (2003), “Sensor Networks: Evolution, Opportunities, and Challenges”,Proceedings of the IEEE, Vol. 91, No. 8, August 2003: IEEE, 1247-1256.

[6]. W. Stallings. Cryptography and network securiy principles and practice. Pearson Education, third edition, 2002

[7]. S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, pages 62–72. ACM Press, 2003.

a. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. SPINS: Security protocols for sensor networks. In Seventh Annual International Conference on Mobile Computing and Networks (MobiCOM2001), Rome, Italy, July 2001.