Energy Efficient & Secured Data Transmission in Wireless Sensor Network-A Review

First Author, Second Author.

Author Details
Sagar.V.Hepat, Computer Science & Engineering, Rajiv Gandhi College of Engineering Research & Technology, India. E-mail:sagarhepat@gmail.com
Prof. R.K.Krishna ,Electronics Engineering, Rajiv Gandhi College of Engineering Research & Technology, India. E-mail:rkrishna40@rediffmail.com

Keywords

Wireless Sensor network, Nodes, cryptographic techniques, symmetric key, asymmetric key, clustering, encryption, decryption.

ABSTRACT

A wireless sensor network (WSN) have many different spatially distributed independent sensors to observe physical or environmental conditions, such as sound, temperature, pressure, etc. and to pass their data to a main location through the network.

Additional Traffic is created with management requests and responses and the data issuing from the network's actual sensing application. Sending and processing the data together, rather than individually can reduce the system's energy.

As the processing of data in WSN consumes more energy. So the data is being transmitted without processing it.

By applying various cryptographic techniques we can transmit the data securely over WSN.

In this paper we discuss the problem with wireless sensor network and have proposed the technique for increasing the efficiency of a node as well as for transmitting the data securely.

1. INTRODUCTION

Each sensor node has a constraint energy capacity in wireless sensor network, so energy-efficient mechanism is important. Sending packets from the source node to the destination node Should be at highest priority than rather sensing the event. A typical node (Berkeley node) in [13] have a configuration of 8-bit CPU (4MHz),128KB flash,4KB RAM and Transmission range of 100 Feet. The nodes in WSN are made of electronic devices that are able to sense, compute and transmit data from physical environments. These sensor nodes have limited energy resources. So, to extend the lifetime of network, energy resources for wireless sensor networks should be managed wisely.

Efficiency of node:-

In wireless communications, energy wastage shortens the networks lifetime. Following are the 4 reasons of energy wastage.

- **Collisions**:-when two nodes transmit at the same time and interfere with each other.
- **Idle listening: -** It happens when the radio is listening to the channel to receive a possible data that is not sent.
- **Overhearing: -** When a sensor node receives packets that are not destined to it. This is the dominant factor of energy wastage, when traffic load is heavy and node density is high.
- **Control:-**packet overhead for protocols to exchange required information.

Security:-

The basic nature of WSN is low power design, which forces security mechanisms to fit under very limiting processing and bandwidth constraints, so security to data has been the challenging issue. The security requirements in WSN are the authentication of entity, message, data, especially in data critical applications. It is observed in [12] that due to Sensor Node Constraints and Networking Constraints in WSN's. Most of the protocols [13][14] are based on Symmetric key cryptography.

2. OVERVIEW OF EXISTING METHODS

This section gives review of the existing techniques for improving energy efficiency of node and provides security to data.

Author in [1] has worked on improving the energy efficiency of the node. By considering some parameters.

A. By Reducing the Communication Costs Radio:

On most wireless sensor network platforms, Communication is one of the key energy consumers. When the data is not been sent or receive. There are different medium access protocols that allow the radio chip to be put into a low power sleep mode (e.g. BMAC, XMAC, and SMAC). Avoiding radio communication saves energy. The conclusions for this observation for a management system were discussed.

1) The management data was sent first, followed by the sensing data after a gap of four seconds.

2) Sending the management data and the sensing data together in a single packet

B. Different Degrees of Co-operative Behaviour:

Either the application or the management framework has to wait for the next packet to be sent, if packets are to be shared between the sensor network application and the management framework. As we have decided that there should be no delay for messages sent by the application.

In this paper [2] Author has focused on reducing the energy wastage during idle listening. The challenge lies in co-coordinating the awake schedule of both sender and receiver. They have designed *Neighborhood-based Power Management (NPM)*, an energy-efficient hybrid MAC protocol that balances synchronization and signaling overhead. In which a sender knows exactly when a receiver is awake either through a priori knowledge of or by synchronizing the wakeup schedules. Thus, senders and receivers wake up at the same time, transmit their data, and then go back to sleep.

Signalling Mechanisms:-[2] All nodes in NPM wake up periodically and poll the channel for activity to receive incoming data messages. Due to the imperfect (out-of-date) synchronization information available to the nodes, NPM must use preambles before the actual data messages, to signal the receivers that they must stay awake until they receive the data messages

Author in this paper [3] has worked on Security of data in WSN. Identity-based attacks are considered the first step in an intruder's attempt to launch a variety of attacks, including denial of service (DoS), session hijacking, man-in-the-middle, data modification, and sniffing. They have proposed 2 techniques.

SOFTWARE-BASED FINGERPRINTING:-Software-based fingerprinting can easily be recorded or extracted using off-the-shelf wireless Devices and existing software. Specifically, by putting the wireless card in monitor mode and using *tcpdump* or *wireshark*, all frames sent over the air can be sniffed. Therefore, the frame/beacon interval, frame size, and source and destination addresses of a frame can be obtained easily.

HARDWARE-BASED FINGERPRINTING:-it is the reflection of defects/unique design of the hardware on the transmitted waveforms.This signature scheme uses the inherent hardware imperfections and characteristics. It is hard to spoof the signature by using off-the shelf wireless devices.

In this paper [4] DES algorithm has been used to encrypt and decrypt data.

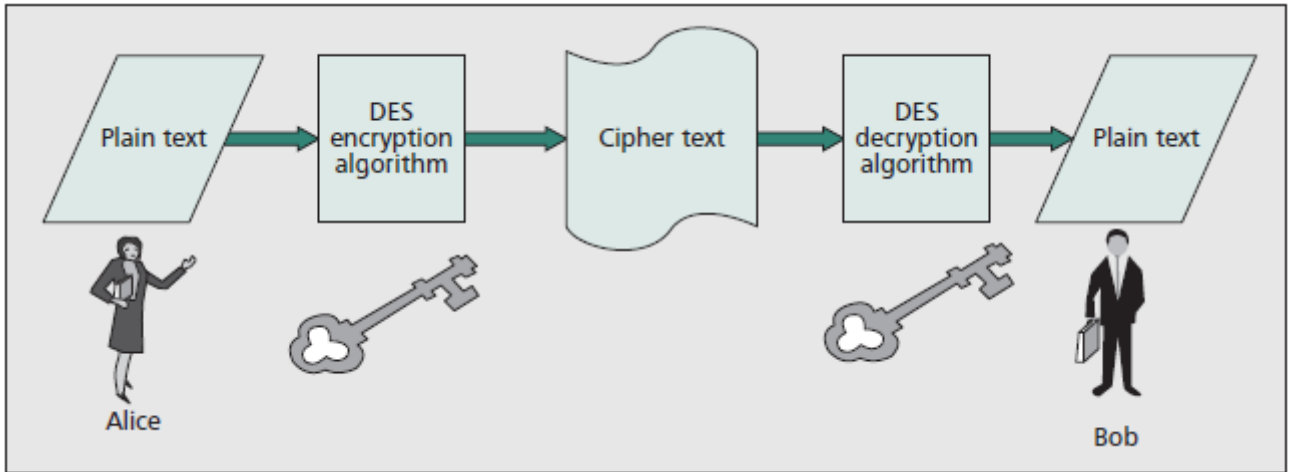

Fig 4:-*The symmetric data encryption/decryption algorithm has been widely used in networks.*

in fig 4:- Alice sends an encrypted message to Bob with a secret key. Bob may use the secret key to decipher the message. Because this message has been encrypted, even if the message is intercepted, the eavesdropper between Alice and Bob will not have the secret key to decipher the message [4].

In paper [5], author has introduced a scheme that could be used to achieve physical layer security against Different attacks. they have classify the existing physical layer security methods into five major Categories: theoretical secure capacity, channel, coding, power, and signal detection approach.

The security services in a WSN should protect the information transmitted over the public channels and the resources from attacks and misbehaviour of nodes. They have proposed a protocol based on RSA.

*Tiny PK***:** Tiny PK security scheme is proposed by Watro et al [11]. The security scheme is used to authenticate the user (external agent) and allows the sensor to share a session key with external agent. The infrastructure requirement for TinyPK is CA, EA and WSN.CA is a trusted Certification Authority, which is an entity with public and private keys.CA is a trusted entity by all friendly units. EA is an External agent is an entity who tries to communicate with a sensor of WSN. Every node is loaded with CA public key while deploying into the network.

3. PROPOSED METHODOLOGY

In this section we have proposed a methodology to increase efficiency of node and a technique to provide security to data.

For increasing the Efficiency of node we are using a protocol i.e., **LEACH Protocol.** LEACH is the earliest proposed single-hop clustering routing protocol in WSN; it can save network energy greatly compared with the non-cluster routing algorithm. In LEACH protocol, all clusters are self-organized, each cluster contains a cluster-head and several non-cluster head nodes, and cluster-head node consumes more energy than non-cluster head nodes. With the purpose of balancing network energy consumption and prolonging the network life cycle, it selects cluster head randomly and each node has an equal chance to be cluster-head [9]. Many other clustering algorithm are

proposed based on LEACH, such as TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol)[6] , PEGASIS(Power Efficient Gathering in Sensor Information Systems)[7] , HEED(Hybrid Energy-Efficient Distributed Clustering)[8]. The cluster structure update constantly and a single updating process are called a round. Each round cycle has two stages: set-up phase and steady-state phase,

- **Set-up phase** is the establishment phase of the cluster:- Each node generates a random number between 0 to 1, and compares this number with the threshold value *T*(*n*). If the number < *T*(*n*), the node is selected as a cluster-head,

The threshold *T*(*n0)* is set as follow;

$$T(n) = \begin{cases} \dfrac{p}{1 - p * (r \bmod \frac{1}{p})} & if\ n \in G \\ 0 & if\ n \notin G \end{cases}$$

Where ***n*** refers the **node identification** in the current sensor network; ***p*** is the **percentage** of cluster-heads; ***r*** is the current **round number**; ***G*** is the set of **nodes that have not been elected as cluster-head in the last 1/p rounds.**

- **Steady-state phase** is the stable data transfer phase, members of the cluster send data to the cluster-head in the way of single-hop during the allocated slot according to the TDMA table, the cluster-head receives all the data from each node in the cluster, fuses all the data into a single signal, after that the fusion signal is transmitted to the base station by cluster-head. Data transmission lasts a certain time, and then the entire network comes into the next round.

For Security of data in WSN:-

For security of data we are using a symmetric key algorithm i.e., RC6 (***R**ivest **C**ipher **6***)[15]. RC6 is a *symmetric key block cipher* derived from RC5.RC6 has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits.

Encryption and Decryption Operation.

RC6 works with four w-bit registers A,B,C,D which contain the initial input plaintext as well as the output cipher text at the end of encryption. The first byte of plaintext or cipher text is placed in the least-significant byte of A; the last byte of plaintext or cipher text is placed into the most-significant byte of D.

We use (A;B;C;D) = (B;C;D;A) to mean the parallel assignment of values on the right to registers on the left.

Encryption with RC6-$w/r/b$

Input: Plaintext stored in four w-bit input registers A, B, C, D
Number r of rounds
w-bit round keys $S[0, \ldots, 2r+3]$

Output: Ciphertext stored in A, B, C, D

Procedure:
$B = B + S[0]$
$D = D + S[1]$
for $i = 1$ **to** r **do**
{
$t = (B \times (2B + 1)) \lll \lg w$
$u = (D \times (2D + 1)) \lll \lg w$
$A = ((A \oplus t) \lll u) + S[2i]$
$C = ((C \oplus u) \lll t) + S[2i + 1]$
$(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

Fig 1:-Encryption Operation in RC-6[15]

Decryption with RC6-$w/r/b$

Input: Ciphertext stored in four w-bit input registers A, B, C, D
Number r of rounds
w-bit round keys $S[0, \ldots, 2r + 3]$

Output: Plaintext stored in A, B, C, D

Procedure:
$C = C - S[2r + 3]$
$A = A - S[2r + 2]$
for $i = r$ **downto** 1 **do**
{
$(A, B, C, D) = (D, A, B, C)$
$u = (D \times (2D + 1)) \lll \lg w$
$t = (B \times (2B + 1)) \lll \lg w$
$C = ((C - S[2i + 1]) \ggg t) \oplus u$
$A = ((A - S[2i]) \ggg u) \oplus t$
}
$D = D - S[1]$
$B = B - S[0]$

Fig 2:- Decryption Operation in RC-6[15]

4. CONCLUSION

Thus we have studied various energy efficiency techniques and have also proposed the protocol used to improve efficiency of node. To transmit the data securely over WSN we have proposed an algorithm i.e, RC6(*Rivest Cipher 6*), which has a key size of 128 bits.

Therefore the proposed technique is an effective approach to improve efficiency of node. And also to transmit data securely over WSN.

Acknowledgment

We would like to thank *Vorugunti Chandra Sekhar, Mrudula Sarvabhatla,*for their help concerning the enhancement of cryptographic techniques over wireless sensor network(WSN).

References

1. Jochen Furthm¨uller, Stephan Kessler, and Oliver P. Waldhorst "Energy-efficient Management of Wireless Sensor Networks" The Seventh International Conference on Wireless On-demand Network Systems and Services IEEE/IFIP WONS 2010.
2. _Farhana Ashraf, Riccardo Crepaldi and Robin H. Kravets University of Illinois atUrbana-Champaign "Synchronization vs. Signaling: Energy-Efficient Coordination in WSN" IEEE/2010
3. kai zeng, kannan govindan, and prasant mohapatra, university of california, davis"non-cryptographic authentication and identification in wireless networks" IEEE wireless communications -October 2010.
4. yi-sheng shiu and shih yu chang, national tsing hua university "physical layer security in wireless networks" IEEE wireless communications -April 2011.
5. Vorugunti Chandra Sekhar, 2Mrudula Sarvabhatla "Security In Wireless Sensor Networks With Public Key Techniques" IEEE 2012.
6. Manjeshwar A, Grawal D.P. TEEN: A protocol for enhanced efficiency in wireless sensor networks[C].Proceeding of the 15th Parallel and Distributed Processing Symp. San francisoi, 2001:2009-2015.
7. Lindsey S, Raghavenda CS. PEGASIS: "Power efficient gathering in sensor information systems[C]". Proceeding of the IEEE Aerospace Conf. NEW YORK, 2002: 1125-1130.
8. Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks [J]. IEEE Trans. On Mobile Computing.2004, 3(4):660-669.
9. LI-Qing GUO, YI XIE*, CHEN-HUI YANG and ZHENG-WEI JING: improvement on LEACH by combining Adaptive Cluster Head Election and Two-hop transmission,[J]. Proceeding
of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, July 2010, pp: 1678-1683.
10. L. Demirkol, C. Ersoy, and F. Alagoz, "Mac protocols for wireless sensor networks: a survey", IEEE Communications Magazine, Vol. 44, Issue 4, April 2006, pp. 115-121
11. R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing sensor networks with public key technology", In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), pp. 59-64, New York, USA, 2004, ACM Press.
12. 12D.W. Carman, P.S. Krus, and B.J. Matt, "Constraints and approaches for distributed sensor network security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood,MD, 2000. 13A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar,"SPINS: Security protocols for sensor networks", Wireless *Networks*, Vol.8 , No. 5, pp. 521-534, September 2002.
13. Jaydeep Sen, "A survey on Wireless Sensor netwrok Security", Technical Report 55-77, International Journal of Coomunication Netwroks and Information Security (IJCNIS) Vol 1, No2 August 2009.
14. P.Jadia, A.Mathuria and Vanstone. Efficient Secure Aggregation in Sensor Networks. In: proc High performance Computing (HiPC), LNCS 3296, pp. 40-49, 2004.
15. Ronald Rivest,M.J.B.Robshaw,R.Sidney,Y.L.Yin " The RC6 Block Cipher" Version 1.1 –August 20,1998.