Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 370 – 379

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

Conservation of energy in wireless sensor network by preventing denial of sleep attack

Swapna Naik[a], Dr Narendra Shekokar[b]

[a]*Department of Computer Engineering, D.J.Sanghavi College of engineering, Mumbai,India*
[b]*Department of Computer Engineering, D.J.Sanghavi College of engineering, Mumbai,India*

Abstract

Wireless Sensor Networks (WSNs) can be used to monitor environments, and therefore have broad range of interesting applications. The applications which may use WSN can be of sensitive nature and therefore might require enhanced secured environment. As sensors are used to monitor sensitive areas therefore Security and energy efficiency is essential consideration when designing wireless sensor networks (WSNs). The Sensor nodes get their power from batteries. Since the sensor nodes are deployed in harsh environment they cannot be recharged. Due to unattended deployment and inability of recharging, the power consumption of the nodes should be optimal. To implement minimum power consumption Sensor networks periodically place nodes to sleep. This is achieved by using the media access control (MAC) protocols. These protocols are designed in such a way that they reduce the energy consumption of sensor nodes by keeping the antenna in sleep mode as much as possible. This leads to power saving. The MAC protocols change the sleep time based on the type of communication required. However, malicious nodes can be introduced in the network and these attackers use their information about the MAC protocol, by manipulating the sleep time of the node, so that life time of the node reduces. This is called as Denial of sleep attack .This paper, addresses the Denial of sleep attack in WSN while at the same time proposing a scheme for authenticating the new nodes which try to change the sleep schedule of the nodes. Only transmissions from valid nodes are accepted. Our scheme uses zero knowledge protocol (ZKP) for verifying the authenticity of the sensor nodes which pass the sleep synchronization messages. Also to enhance security further the interlock protocol is used during key exchange. The paper presents a detailed analysis for various scenarios and also analyzes the performance while implementing this secure authentication.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: Wireless Sensor Network, ZKPAuthentication, Public Key Cryptography, Denial _of _sleep attack, WSN.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.164

1. Introduction

Sensor nodes which are used to build sensor networks have limitations in terms of resources such as storage, computational and communication capabilities. Sensors also have a limited cost, as their nodes are small and cheap to build so a large number of them can be used to cover an extended geographical area. The network built using many small and cheap sensors has given rise to exciting new applications in several areas of our lives. Sensors can be used when monitoring our environment, animal habitats, healthcare applications, home automation, and traffic control. However, like all networks, sensor networks are susceptible to security threats which, have to be defended well, otherwise application of sensors in various critical scenario is not possible. Since communication in sensors is wireless and they have limited battery power the use of security measures employed in other networks is infeasible. This has created a large number of vulnerabilities that attackers can exploit, in order to gain access to the network and manipulate them [17]. The key factor one must keep in mind when designing wireless sensor network application are energy efficiency of MAC protocol. The MAC protocol must keep the radio in a low-power sleep mode as much as possible [1].

The denial-of-sleep attack is a specific type of denial-of-service (DoS) attack that targets a battery-powered device's power supply resulting in quick exhaust of this constrained resource. It is hard to replace those sensors which fail on account of their battery drainage. It is also difficult to recharge those sensors. Thus to effectively increase life of individual sensor nodes and in turn the whole sensor network the battery charge carried by these nodes must be conserved . If we fail to stop the attack, the network lifetime can be reduced from months or years to days [13]. To prevent this attack we have to authenticate nodes which are going to change the sleep time of the nodes so only synchronization messages coming from authenticated nodes are accepted.

Whenever authentication is carried out using symmetric keys and hash functions the security of the WSN nodes can be compromised. Any malicious node who can gain access to the symmetric keys can access the information belonging to the Base Station. When base station data is in the hands of malicious nodes the entire WSN stands compromised. This problem can be dealt with by using challenge response protocol.

In challenge based authentication the claimant has to disclose his original identity to the verifier to prove it. In such a situation if the verifier is vulnerable, whatever information is received from claimant node by the verifier can be accessed by malicious user node too. Once this information is available the attacker can prove himself to the verifier and gain access to sensitive data. In sensor networks Base Station is a critical resource, therefore it has to be protected .Any data belonging to Base Station should not be known to other nodes .This data can be used by an intruder to act as Base Station and collect all the data's from all Cluster Heads. In Zero knowledge based authentication, the secret of the claimant is never revealed directly, instead the claimant's secret key is used to calculate a value which can be used in interactive manner between the claimant and verifier to carry out authentication. The zero-knowledge proof protocol is a powerful cryptographic technique which uses a challenge from the verifier making it difficult to break. Therefore it can be applied in many cryptographic applications and operations such as identification, authentication, key exchange and others [4][5] . In this paper an effective solution to defend against Denial_of_sleep attack on a sensor network using zero knowledge protocol based on the principle of Fiat_Shamir exchange is proposed.

Obstacles to sensor security

When designing a secure sensor network numerous obstacles have to be overcome .The main hurdles in sensor security are discussed below.

1) Unreliable Communication**:** Another threat to sensor security is unreliable communication. The security of WSNs depends heavily on a user's security protocol that is again dependent on communication. Another cause of damaged packets is the unreliable wireless communication channel.
2) Unreliable Transfer: The routing protocols used in a wireless sensor network are packet-based, and these routing protocols are connectionless, hence inherently unreliable. Due to channel errors, packet may get damaged or may be dropped in the path because of highly congested nodes. The results are lost or dropped packets.
3) Conflicts: Considering the communication channel to be reliable, there may be a case that the communication itself is unreliable. The reason behind this is the broadcast behavior of the wireless sensor network.. This can be a major problem in case of high dense sensor network [6].

4) Latency: Latency can be increased due to network congestion, multi-hop routing and node processing, which will make it difficult in achieving synchronization among sensor nodes. The synchronization issues can make it hard for maintaining sensor security as security mechanism depends on critical event reports and cryptographic key distribution [7].
5) Unattended Operation: The sensor nodes may be left unattended for a long period of time which depends on function of the particular sensor network.
6) Exposure to Physical Attacks: Since sensors are deployed in an environment which is open to adversaries, and also open to different physical condition like bad weather and so on. There are always potential risks that a sensors may suffer a physical attack.
7) Managed remotely: The sensor network is managed remotely, making it impossible to find or detect physical tampering (like tamper proof seals) and physical maintenance (like replacement of battery).
8) No Central Management Point: A sensor network is distributed network, which does not have a central management point. This property will increase the vitality of the sensor network. However, if it is not designed correctly, it will make the network organization difficult to manage and Inefficient. [15][16].

Security Issues for Wireless Sensor Network

The flexible mesh architecture of WSN can dynamically adapt to support introduction of new nodes or be expanded in order to cover a large geographic region. This network is flexible but introduces new issues in the communication process; some of these issues are discussed below.

1) Data Confidentiality: Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighbouring networks.
2) Data Authenticity and Integrity: One can easily inject malicious data in sensor network. So receiver should sues make sure that data it received is correct and legitimate data as in this malicious data can lead to wrong interpretation by receiver.
3) Data Freshness: Data freshness implies that the data is recent, and it ensures no old messages are replayed over network. For this counter must be used that can determine freshness.
4) Availability: Availability ensures that services and information can be accessed at the time they are required.
5) Data Confidentiality: Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighbouring networks.
6) Data Authenticity and Integrity: One can easily inject malicious data in sensor network. So receiver should make sure that data it received is correct and legitimate data as in this malicious data can lead to wrong interpretation by receiver.

The paper has been organized into the following sections. Section 1 introduces the topic while discussing the open issues in WSN security. This section also discusses covers the various obstacles posed to sensor network security. Section 2 discusses the background and related work .providing a brief overview of the related work that has been carried out on the topic. Section 3 explains the proposed system. Section 4 shows Simulation Experimental setup and step by step procedure. Section 5 carries out the analysis of the results. Finally, section 6 concludes the paper.

2. Background and Related Works

WSN have inherent security risk due to broadcast nature of communication. Denial of sleep attack can cause the networks doom in few hours. Therefore proper authentication to prevent malicious node attack is imperative. The research on sensor network security is critical as sensor network can be used in critical health monitoring, in pacemakers in human heart also in surveillance and defence applications.

David R. Raymond et al [13] classifies denial-of-sleep attacks on WSN MAC protocols. Secondly, it explores potential attacks from each attack classification, both modeling their impacts on sensor networks running four leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks on these protocols.

Manju.V.C et al [1] in her paper Proposed method to defend denial of sleep attack the method consists of two parts, Network organization and Selective level authentication. Kyung Choi et al [2] in the paper uses zigbee for security advanced encryption standard (AES) algorithm, adds to a security model provided by IEEE 802.15.4.

Martin Peres et al [10] suggests generating a secret key by deriving an already-shared key, this is called key derivation, network given a unique big random identifier that would be shared by all the nodes of this network. L.Sujihelen et al [20] in his paper carries out authentication using Virtual Certificate. A global authority will provide an initial trust between nodes. This is done by creating and verifying certificates.

Jayanthiladevi et al [3] has further improved on the above by suggesting that secured communication can be realized using user authentication concept but also points out that public key cryptography is used when there is large number of user due to its scalability. Here sensor communicates among each other with the help of symmetric cryptography. The user and timestamp's validity is verified by the gateway node.

Mahmood Khalel et al [12] points out Diffie-Hellman algorithm are vulnerable to the man-in-the-middle attack in which the attacker is able to read and modify all messages between Alice and Bob. The man-in-the-middle attack can be prevented by a station-to-station key agreement by using digital signature with public key certificates to establish a session key between Alice and Bob.

Siba K. Udgata, Alefiah Mubeen [9] in their paper use the s-disjunct code matrix. Each column in the matrix corresponds to codeword of each node. Base station maintains data structure corresponding to every sensor node, and their fingerprints. If ZKP verification is true then the prover is authenticated and later verified for k times to validate it else the base station is alerted about the compromised prover node.

L.B. jivandham et al [6] proposed security protocol which integrates one round Zero Knowledge Proof and AES algorithm for node authentication, where only authenticated nodes will be accepted during node-move-in operation.

Dr. D. S. R. Murthy, B. Madhuravani, G. Sumalatha [26] survey Key establishment protocols in various flavors. This Paper discusses the following key exchange methods Key Exchange with Symmetric Cryptography, Key Exchange with Public-Key Cryptography, Key Exchange Authentication Protocol and Shamir's Three-Pass Protocol which enables 2 parties to communicate securely (over 3 message exchanges) with each other without the need for any advance exchange of either secret keys or public keys .The comprehensive study on different asymmetric authentication protocols with detailing of benefits and problems with asymmetric key distribution algorithms is the beneficial to the user. This paper does not reach any conclusion regarding the best method. All algorithms have their pros and cons. So based on our application we need to choose the suitable authentication and key exchange method.

To overcome the weaknesses of the Siba K. Udgata, Alefiah Mubeen [9]scheme, we propose security and energy improvements in our paper. The proposed security improvements can easily be incorporated into the Siba K. Udgata, Alefiah Mubeen [9] scheme to implement a better way to prevent the denial of sleep attack in WSN. Furthermore we have implemented a better way of transferring keys initially by using the interlock protocol.

3. Proposed System

Our proposed system architecture is as shown in Fig 1 .System consists of the Base station (BS) ,Cluster head (CH) . There are some nodes under each of the Cluster heads. The Base Station is connected to the internet. A network consisting of around 8-12 nodes will be used including the attacker node, the sink node, the CA node and the BS node.

A: Attack Scenario

The attack will be implemented on SMAC protocol for demonstration of denial of sleep mechanism. The attack that will be implemented will be replay attack there will be around 4 rounds of ZKP execution as per requirement Selective Local Authentication will be used for detection of denial of sleep attack; hashing and interlock protocol will be used for key exchange and Zero Knowledge for authentication of base node.

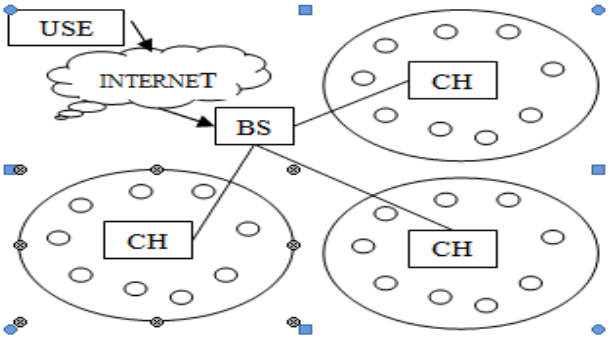

Fig.1. Base station and cluster head

The transfer of keys from the base station to other nodes is critical task as keys can be exposed to man _in_the middle attack; to protect against man in the middle attack the key transfer takes place by using the interlock protocol where the key encryption is done using the AES algorithm.

In the interlock protocol the encrypted key is divided into two parts one part is transferred at one time while the second part is transferred after getting response from the receiving node only on joining the two parts can the key be decrypted at the receiving base station .To carry out this transfer the nodes joining any network must agree on some symmetric key encryption technique. Here we have used the AES algorithm which divides the encryption into two parts. These two parts are sent one after the other by first authenticating the transfer is to the right nodes.

In sensor networks the sleep period of the nodes is regulated by the MAC protocols. These MAC protocols work by sending synchronization signals to regulate the sleep period of the nodes. These protocols work by using a lot control messages like request to send (RTS) and clear to send (CTS) called as synchronization (SYNC) packet. An effective way to carry out a Denial_of_sleep attack is replaying control packets, like RTS messages. This prevents nodes from sleeping and results in wasted power. If these messages are sent within a small time gap then nodes in the network do not have time to transition to sleep mode and back again. This results in loss of battery power. This loss can be forced on all nodes within transmission range of the attacker .The attacker sends SYNC messages which indicates to nodes when the sending node will next enter the sleep mode.

Whenever a node receives a SYNC packet from another node on the same sleep schedule as itself, it recalculates its next sleep time to maintain synchronization. In sensor network nodes do not simply reset its next sleep time and the time in the received SYNC packet as follows:

New sleepTime = old sleepTime + receivedSYNCpkt.sleepTime /2

This method does not change the sleep schedule drastically whenever a SYNC message is received, it infact allows nodes on the same schedule to improve synchro-nization gradually over time. A Denial_of_sleep attack can be executed by replaying SYNC packets. Even if these packets are encrypted, an attacker watching the network can identify these packets easily. This is possible by an attacker monitoring all messages by their size and timing. For example S-MAC SYNC packets are 10-B long and occur during the first few milliseconds of an S-MAC frame. Once the attacker gains this information he can easily manipulate these packets even though they may be encrypted. So we are using authentication to protect the network against these attacks.

B: *System Flow*

For deploying the nodes in the network and for authenticating them as valid nodes, we generate unique public, private keys for communication for each sensor node.

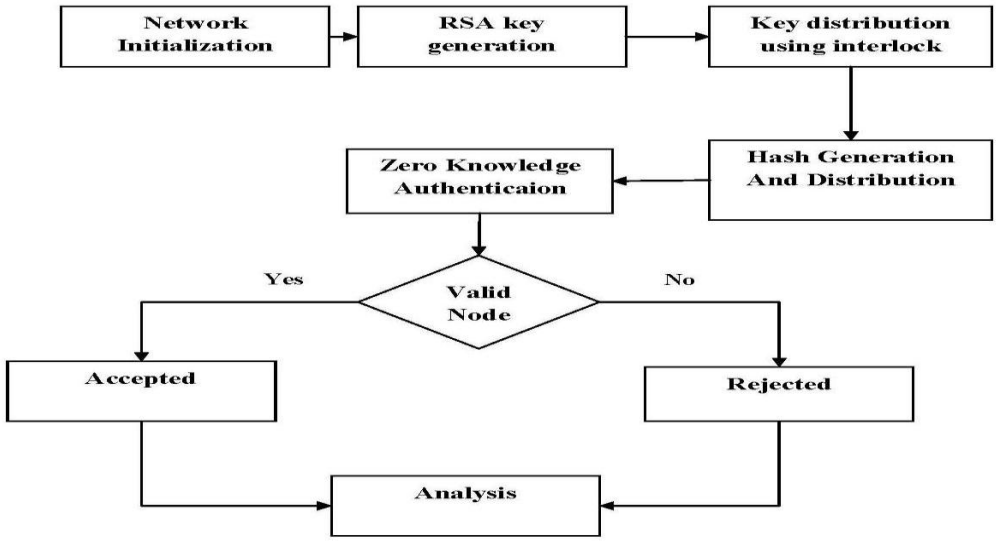

Fig. 2. System flow

This is done by using the RSA algorithm for key generation. The keys can be exchanged by using the interlock protocol for protecting this communication against man in the middle attack.

Our proposed system architecture is as shown in Figure 1. Base station stores and has access to information of all sensor nodes which includes the cluster heads as well as all nodes under them. When we are authenticating the nodes the base station acts as the third party for negotiation. The node sending the sleep synchronization messages is the prover and receiving node acts as verifier. The system flow happens as shown in Fig. 2. Each of node has a unique private key which is used as a private key in this case called s. The Prover and verifier share the public key. In the process of authentication base station transmits the secret key of the prover from the base station when it is requested by verifier. Instead of directly passing the key, base station calculates a value $v = s^2 \bmod N$ .Here s is private key and N is public key. The value of v is given to the verifier when it requests for the same. When we use Zero knowledge protocol (ZKP) for authentication using a number of verification rounds, there is a possibility of guessing the random numbers. When we execute ZKP with each round of zkp this possibility of wrong authentication is reduced at each round by 50%. The private key s remains private in domain of the prover and thus remains a secret. This makes it difficult to derive s from v given $v = s^2 \bmod N$.

4. Simulation Experiment

The simulation is accomplished on a ns2 environment. First we setup a virtual machine VMware Workstation on linux. We use a set of eleven nodes. The nodes update their sleep schedule using SMAC protocol .AODV routing is used during simulation. The simulation period is 50ms.Initial energy of each node is 1000 milliwatts . The channel used in simulation is wireless channel.MAC protocol is SMAC. The idle power is set to 0.014 milliwatts, receiving power is 0.014, transmitting power is 0.036, and power required by sleeping nodes is set as 0.000015milliwatts.Power required during transition from one state to another is 0.028 milliwatts.

In this simulation base station is generating the keys using the RSA algorithm. The system is implemented in the steps.

1. Node 10 will generate a unique numeric secret key for each sensor node and update it to each node except the attacker Node 7.
2. numeric public key N will be generated by Node 10 and given to Node 11
3. This public key will be transmitted during communication between Node 0 and Node 9.This transfer is by using the interlock protocol.

4. Node 0 is prover and receiving (sink) node 9 verifier.
5. Secret key of Node 0 from Node 10 will be requested by node 9.Instead of directly transferring v is transferred instead of s.
6. Node 10 will generate a secret code v = s*2 mod N (where s is secret key of Node 0 and N is the public key).
7. The value of v is given to Node 9 on its request.
8. The hash of the public key N will be used during key transmission from Node 10 to Node 0 or Node 9 to validate Node 2 which will be maintained by Node 11.
9. The hash of the public key N of the Node 10 will be distributed by the Node 11
10. This hash will also be sent by the Node 10 along with the keys to Node 0 or Node 9.
11. On successful validation of hash data only will the node accept the keys from the Node 10.
12. The Node 7 will have invalid secret key as compared to key of valid Node 0 of which packet is being replayed. Hence, the secret code received from Node 10 for Node 0 and Node 7 will mismatch, thereby leading to detection of the attack.

5. Result Analysis

For the result analysis we have created three graphs. In the graphs shown in Figure 3, Figure 4 and Figure 5 in these graphs the x_axis shows the simulation time the y_axis shows the battery energy, packet delivery ratio and the throughput respectively.

The graph in Figure 3 shows the usage of battery power during simulation. When the attack takes place the red line shows that the battery of the node attacked quickly goes down as the replay message synchronizes the sleep cycle again and again thus depleting the battery life very fast. The battery life of the network shows vast improvement whenever the attack is prevented by carrying out the zero knowledge authentication for nodes sending synchronization messages. The black line in figure 3 shows that preventing the attack improves the lifetime of the sensor network significantly

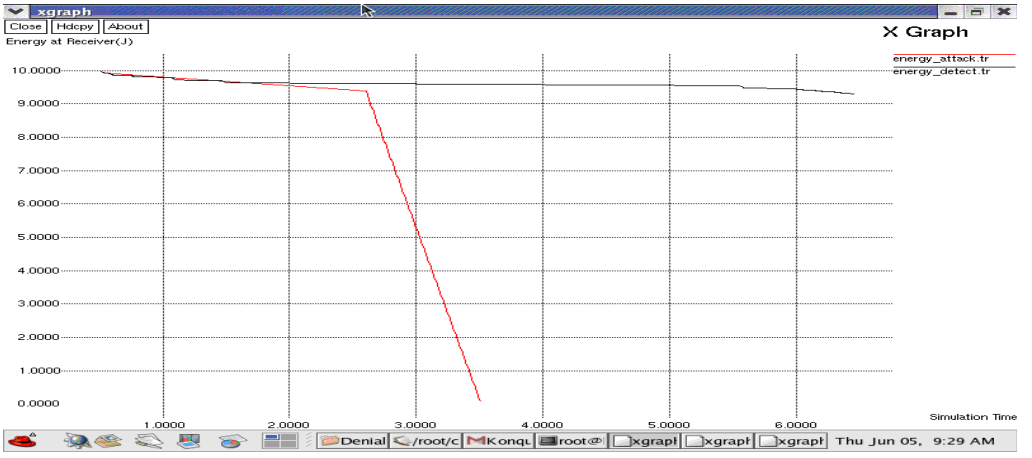

Fig.3. Energy analysis with and without attack

The comparison of packet delivery ratio with and without the attack shows an improvement of performance when the attack is prevented. The red line shows attack scenario where there is high packet delivery initially as packets are replayed repeatedly by the attacker node but once the battery is depleted sharp drop in packet delivery is seen.

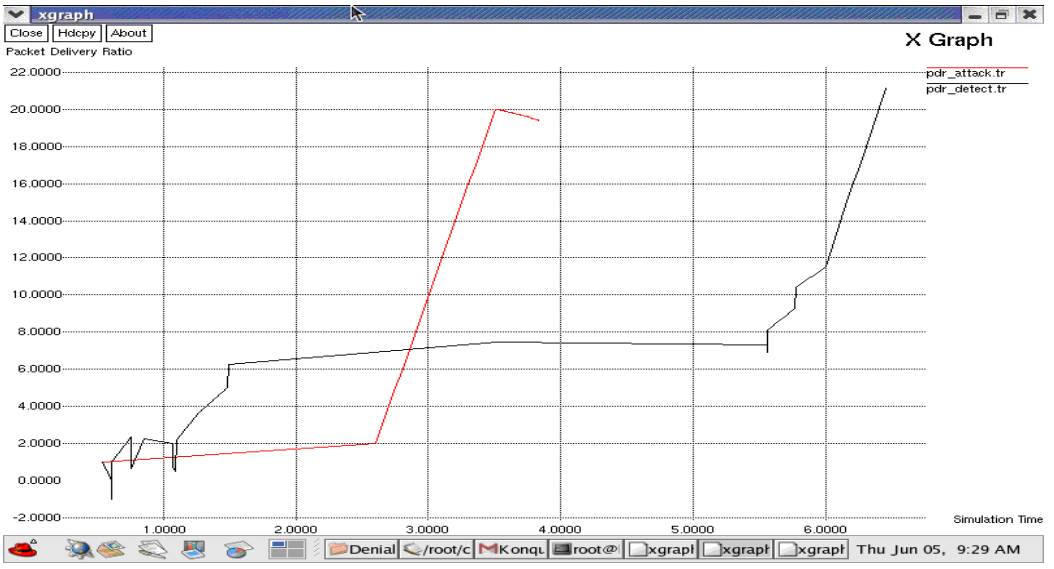

Fig.4. Packet delivery ratio with and without attack

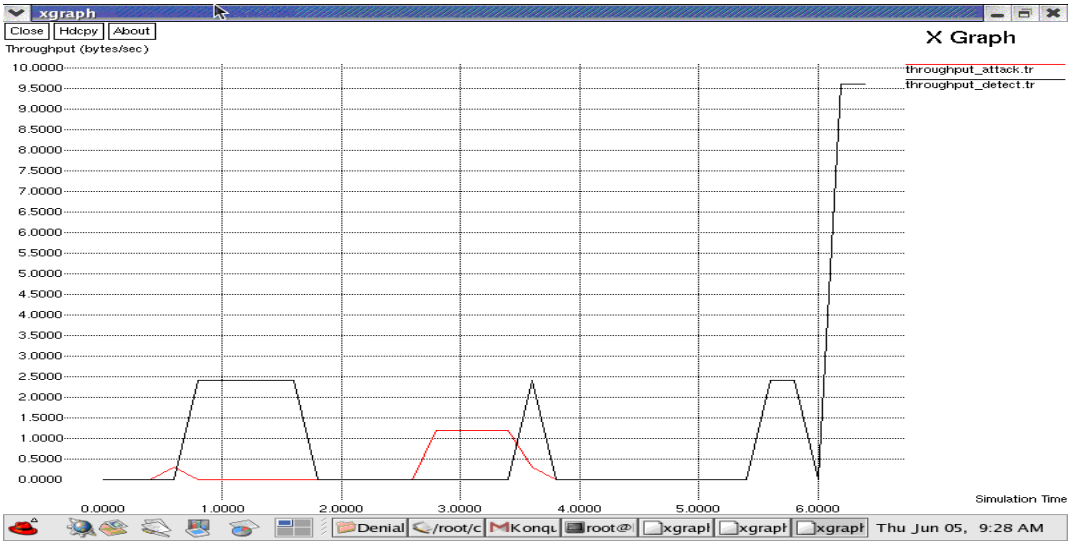

Fig.5. Throughput with and without attack

The improvement in throughput when the attack is prevented can be seen from the graphs above.

6. Conclusion

In this paper, we have detailed our proposed defending mechanism against the denial of sleep attack. This solution is an effective method for preventing this attack as all the nodes sending the synchronization messages will be validated before those messages are accepted and rejected if the node is not validated. The attacker node cannot replay the sleep synchronization signal again as its sleep schedule will not be accepted without authentication

Sensor nodes have limited capabilities and resources. More importantly excessive use of resources may result in a decrease in network lifetime. The mechanism against the denial of sleep attack is authentication of node trying to send synchronization message. This is done by using zero knowledge protocol. By preventing the denial of sleep attack we see significant improvement in network life time the x -graph analysis shows the same.

This method of defence extends the network lifetime effective use of battery power while communicating securely within the network. A novel security framework that provides a comprehensive security solution against the vulnerabilities of WSN has been proposed. The zero knowledge protocol used in combination with the interlock protocol for key transfer is capable of preventing man in the middle attack and replay attack. This also consumes less resource and is suitable for providing fool proof security in WSNs.

References

1. Manju.V.C , Senthil Lekha.S. L. , Dr.Sasi Kumar M. “Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks”, Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT2013)
2. Kyung Choi, Minjung Yun, and Kijoon Chae “An Enhanced Key Management Using ZigBee Pro for Wireless Sensor Networks “, 2012 IEEE399 ,ICOIN 2012
3. Merad Boudia, Omar Rafik , Feham Mohammed ,“The impact of ECC's scalar multiplication on wireless sensor network”, 17978-1-4799-1153-0/13/$26.00 ©2013 IEEE
4. Erfaneh Noroozi I ,Javad Kadivar, Samira, Hasani shafiee, “Energy Analysis for Wireless Sensor Networks” 201O 2nd International Conference on Mechanical and Electronics Engineering (ICMEE 2010)
5. David R. Raymond and Scott F. Midkiff Bradley , “ Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks” 2007 IEEE
6. Mircea Frunza', Luminita Scripcariu ,”Improved RSA Encryption Algorithm for Increased Security of Wireless Networks” 1-4244-0969-1/07/$25.OO ©C2007 IEEE.
7. Nivedita Datta, “ Zero Knowledge One Time Digital Signature Scheme”, Proceedings of 2012 IEEE International Conference on Computational Intelligence and Computing Research
8. B.Vijayalakshmi ,”A Zero- Knowledge authentication for Wireless Sensor Networks based on Congruence “ , IEEE-ICoAC 2011
9. Siba K. Udgata, Alefiah Mubeen ,”Wireless Sensor Network Security model using Zero Knowledge Protocol ”,publication in the IEEE ICC 2011 proceedings
10. Martin Peres , Mohamed Aymen Chalouf & Francine Krief, “On optimizing energy consumption: An adaptative authentication level in wireless sensor networks” 978-1-4577-1261-6/11/2011 IEEE
11. Xiaojiang Du ,Yang Xiao, Mohsen Guizani & Hsiao-Hwa Chen , “Defending DoS Attacks on Broadcast Authentication in Wireless Sensor Networks” 978-1-4244-2075-9/08/$25.00 ©2008 IEEE,publication in the ICC 2008 proceedings.
12. Mahmood Khalel Ibrahem , ” Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof “, 2012 International Conference on Future Communication Networks
13. David R. Raymond, C. Marchany, Michael I. Brownfield and Scott F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols”,IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009 367
14. Song Ju ,” A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography “978-1-4673-1332-2/12/$31.00 ©2012 IEEE
15. Rakesh Maharana,”An Improved User Authentication Protocolfor Hierarchical Wireless Sensor Networks using Elliptic Curve Cryptography” Department of Computer Science and Engineering
16. National Institute of Technology Rourkela Security Requirements in Wireless Sensor Network IJSER International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 2213 ISSN 2229-5518 IJSER © 2013
17. Jos´e Rafael Trigueiro de Carvalho,” Comparative analysis of authentication schemes on a Java Card smart card”,Dissertation submitted for obtaining the degree of Master in Electrical and Computer Engineering.
18. Amanjot Kaur, ”Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method” ,International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 2212 ISSN 2229-5518 IJSER © 2013
19. K.Gomathi , T.P.Senthilkumar ,” A Study on Security Challenges in Wireless Sensor Networks: Key Management Approaches “,International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 9– Sep 2013
20. L.Sujihelen , Dr. C.JayaKumar, “Authentication Solutions For Wireless Sensor Network Based On Virtual Certificate Authority “2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]
21. Jayabhaskar Muthukuru, Prof. Bachala Sathyanarayana ,Prof Sri Krishnadevaraya ,”Implementation of Elliptic Curve Digital Signature Algorithm Using Variable Text Based Message Encryption “.
22. IshwaryaMathi Manickavasagam1, MadanMohan Anbalagan, Sivasankar Sundaram,” Secure And Efficient Key Pre Distribution Schemes for Wsn Using Combinatorial Design”. IJRET,Volume: Apr-2014.
23. Dr. D. S. R. Murthy, B. Madhuravani, G. Sumalatha,” A Study on Asymmetric Key Exchange Authentication Protocols”,

International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012

24. Shakhov V., Popkov V., "Performance Analysis of Sleeping Attacks in Wireless Sensor Networks", International Conference on Computational Technologies in Electrical and Electronics Engineering, IEEE REGION 8 SIBIRCON 2008.
25. CrossBow Corporation, MICA2 and MICAZ Series Data Sheet [Online], http://www.xbow.com
26. J. Kahn, R. Katz, and K. Pister, "Next century challenges: mobile networking for 'Smart Dust', " In ACM MobiCom , Aug. 1999.
27. Xin Luo, Teik Guan, "defeating Active Phishing Attacks for Web-based transactions", International Journal of Information Security and Privacy, 1(3), 47-60, July-September 207
28. G. Padmavathi , D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" ,(IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009