International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

SNPDAC: Secure Network Protocol with Data Access Controlling in WSN

Uttarkar Amit Ratikant[1], Hingoliwala H. A.[2]

[1, 2]PG student JSCOE, JSPM, Pune Associate Professor, JSCOE, JSPM Pune

Abstract: ***Secure communication refers to exchange of information in encrypted form, so that adversary or unauthorized party could not access the sensitive information. In Wireless Sensor Networks (WSN) due to resource limitations security and privacy becomes very key issue as each of sensor nodes collects sensitive information and transmits over the network. Since Sensor networks does not support the traditional security mechanisms we have concentrated on data access control more precisely in order to avoid data leakage or unauthorized party. Here we are discussing the issue of data access control in WSN with help of Key-lock match method to prevent unauthorized access to data reports. Along with the real time implementation we are detecting replay attack considering some traditional cryptographic methods. Results show that we achieve higher security than the existing methods.***

Keywords: Sensor Nodes, Replay attack, Buffer filter

1. Introduction

A WSN can be defined as a network of devices, denoted as *nodes*, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links [2]. Wireless sensor networks (WSN) are interesting entities for scientists and engineers. WSN can assist scientists and engineers to collect important data about various phenomena at the fraction of the cost of conventional data acquisition systems. However, the level of technical knowledge required to program and deploys the WSN nodes to acquire such useful scientific data. Security of Sensor network is also one of the key issues as Sensor network nodes can physically captured or destroyed. Sensor networks are vulnerable to security attacks due to the broadcast nature of transmission. Hence one could think that various security mechanisms which are available for computer networks are also applicable to WSNs. But it's not possible; in fact there are totally separate protocols and different approaches used for handling security in WSNs. As Sensor network's node had constraints like low life battery, lower CPU power, less memory storage etc. as well as network had constraints like wireless in nature, it might be ad-hoc, unattended etc. the special considerations are taken into account while developing the security protocol for WSNs. Already there are lots of protocols and technologies that have been working on security issues of Wireless Sensor Networks. [Explained in section II].Inspiring by these issues I am presenting the SNDAC a security protocol based on data access control in Wireless Sensor Network.

2. Related Works

Wireless sensor network has many resource constraints as compared to the traditional computer networks. Due to these resource constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms which borrow the ideas from the current security techniques, it is necessary to know and understand these constraints first. One typical sensor network consists of nodes, small battery powered devices, which communicate with more powerful base station, which in turn connected to the outside network. There are several state-of-the-art protocols and algorithms, which all are doing a satisfactory job of securing internet communication. However these protocols and algorithms are too heavy weight for use in sensor network. They are having very high communication overheads and they are not designed to run on computationally constrained devices. They will also increase power consumption. Hence there is a need for new more energy efficient cryptographic algorithms and protocols.It's not the case that the security protocols for Sensor Networks are yet not having been developed whereas there are various research and development already going on secure network protocol for WSNs.

Some technologies have been developed, including SPINS [3], TinySec [4], ZigBee [5], and MiniSec [6]. SPIN is a data-centric routing protocol. It achieves lower energy consumption by keeping a consistent counter between the sender and receiver, and hence an initialization vector (IV) is not required to be appended to each packet. On the other hand TinySec encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted. TinySec achieves low energy consumption by reducing the level of security provided. MiniSec is a secure network layer that obtains the best of both from TinySec and ZigBee: low energy consumption and high security [6]. It achieves low energy consumption by appending a few bits of the IV to each packet. Kun *et al.*'s[7] had proposed having three stages in it guarantee that all traffic in the system is authenticated, as well as revoke compromised nodes and update group key but method is unable to defend or detect replay and jamming attacks. Here we are concentrating on secure packet transmission and attack detection based on algorithmic strategies used in system. Our system is based on proposition that data will be forwarded in encrypted form from source to destination. Adversary or attacker will try to duplicate the packet when they are received and forward to next node on path. It seems to be on same path and within same network cluster area. As we are developing system on real time based communication approach, we are assuming Data access control matrix for static network instead of dynamic form. When fully implemented on Java platform

result show that system can transfer packets from source to destination in proper fashion with adequate time. It also detects replay attack and via algorithmic approaches used for it. System is providing practical security for files and reports stored on sink node (sender node). From analysis we can say it's an efficient security mechanism from others existing protocols.

3. Proposed Method

A. System Design Approach

The proposed system is developed on java platform and based on real time application. We are not using any simulator to simulate the packet transmission and attack detection. Here we base our design to AES encryption standards. AES has been proven as most suitable block cipher for WSNs [8] [9]. There are various authentication schemes proposed for wireless sensor networks. We are using CFA- Constrained Function based Authentication [10] with some modification for our proposed system. When any node u want send message/files/data to destination node u, it calculates Message Authentication Code. This MAC is associated with perturbation which is randomly selected. According to modified AES, packet has header, source address and destination address and initialization vector, encrypted message, MAC and send to node v possibly through a multi hop (in our case through intermediate node) path. At Destination side when packet is received it calculates verification difference. If the verification difference is within range then authenticity and integrity of Packet is successfully verified. Otherwise packets are discarded.

B. Data Access Control

For Memory Data Access control we are using static access control matrix in the code module. This matrix is responsible for the handling the files or data on sever side/ sink side. In access matrix we are having the user ids at rows and file id's at columns. When any user request for file, he has to enter the valid User ID and File ID he want to access. If valid pattern request found then it will send the file requested in encrypted form on network path. This refers to normal packet transmission where data or packets were not duplicated. If same scenario is followed and instead of normal intermediate node if it becomes the adversary or attacker then there will be slight different approach. In such case it will duplicate the file received from previous node on path. Thus it might be possible that internal node its self-get compromised. Detection of such thing is very important and we are using packet marking algorithm for the detection of source of the adversary or attacker, in our case we are showing this at intermediate level on network path we had assumed.

C. System Architecture

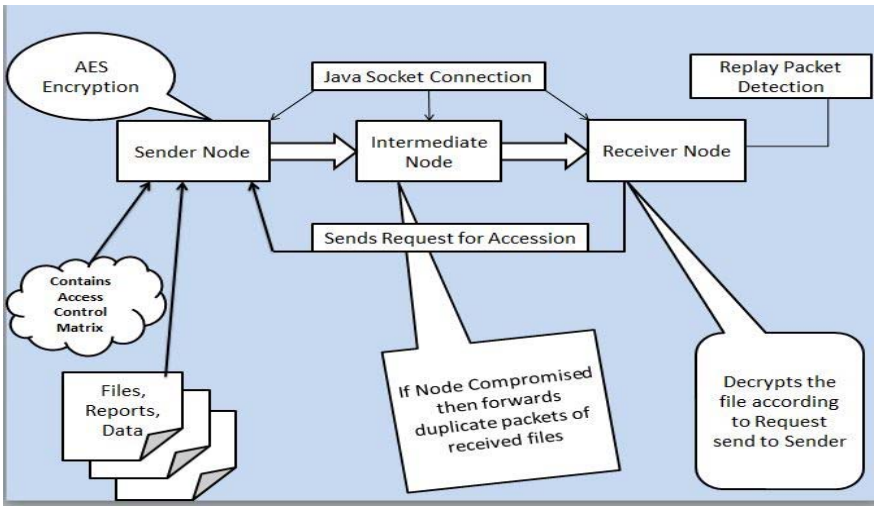

Figure 1: Proposed system Architecture

Figure 1 shows proposed system architecture of SNPDAC. At sender side we base our design AES encryption standards. Various reports file had been placed on it. It is also responsible for validating any malicious request for the files and reports. If file requests are valid it will encrypt the file and send it to requester on Java's socket connection. Once established socket connection will work for retrieving request and in second run it will transmit the file to next node in the system. When file is received at receiver it will acknowledge it by sending acknowledgement to previous node. At receiver we are having option for file decryption according modes we had requested. If the intermediate node gets compromised internally by somebody as an attacker then it will duplicate the packet and forward it. Therefore at receiver we are trying to detect replay attack. If replay packets are detected then buffer filter used in system will drop or discards the packets.

D. Algorithmic Strategy

In this section we are going to discuss the algorithmic strategy used for our proposed system. As we know that the system is based on real time implementation basis we are using different approaches for our prosed work. In proposed work we are using constrained function authentication in modified form for data transmission. Following algorithm is used for secure data transmission from source to destination. It is also responsible for calculation MAC address and for detecting replay packets on system.

Algorithm: Data transmission & Replay attack detection.

Input: Packet M

Output: Result of operation

1. Calculate Message Authentication Code based on encryption based on AES.
2. MACu(v,msg)=authu(v,Ku,v,h(msg))+nu,s. where nu,s is randomly picked from[0, 2^{r-2} -1].
3. Send packet M= (Header, u, v,Eku,iv(msg), MACu(v,msg))
4. At Intermediate node on receiving packet M It will calculate Verification difference If VDe,u € [0, 2^{r} -1] then Forward & return True otherwise Drop M
5. At Destination Node v on receiving packet M Check Buffer Filter for replay packets If replay packets. Drop the packets
6. Exit.

For access control mechanism as said before we are using static matrix which is already feed into system. In existing work [1] we are having algorithm based on dynamic wireless sensor network where users and files adding and removing process is performed dynamically.

4. Evolution and Results

In this Section we are going to concentrate on performance analysis of our proposed system. Aim of SNPDAC: Secure Network Protocol and Data Access Control to provide practical high security which will transmit data in encrypted fashion based on AES. Thus we are concentrating on replay attack detection as well as file access modes to be provided. If particular user request file its request is validated and according to access mode of file accession file will be transmitted to requester. Using the theoretical aspect we are controlling accession of data stored in node memory by using rules of accession. We are obtaining our results in terms of various factors as discussed below in graph and tables

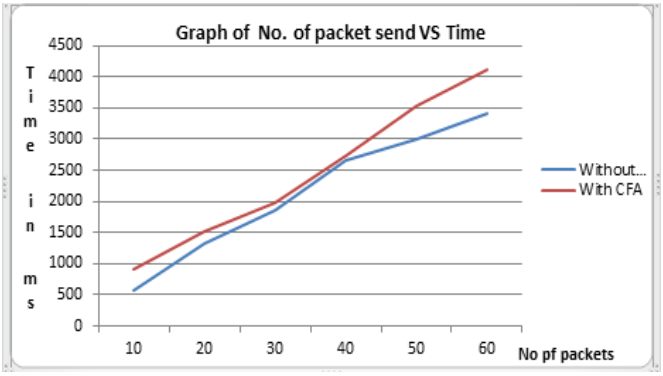

Figure 2: No. of packet vs. time

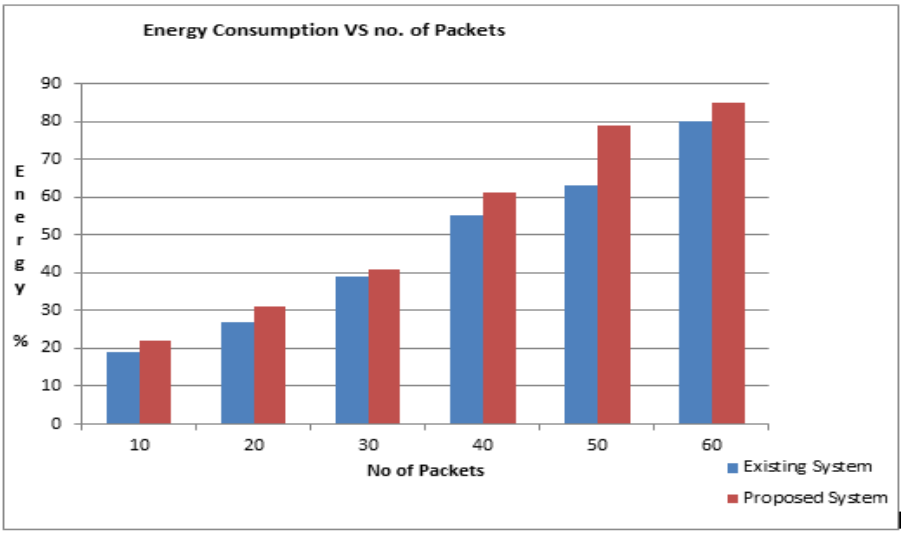

Figure 3: No. of packet vs. energy consumption

Another result we are obtaining is based on energy consumption verses number of packets transmitted over the network path. Clearly it show that proposed system will consumes less energy as compared to existing system.

5. Conclusion

In Sensor node energy consumption and node compromised by an attacker or adversary who can get access of sensitive information or files or reports which are transmitted over network path are very serious issues. Since Sensors networks are dynamic in nature handling the security mechanism on them also tedious. There have been lots of existing technologies or protocols which have been proposed for WSN's security and prevention of it from the attacks. Our proposed system SNPDAC establishes practical high security on data to be transmitted in air form (wireless form) and it has also a filtering capability to permit or deny data access based upon a set of rules, which used to protect the data from unauthorized access while permitting legitimate communications to pass on network path. Our system is able to detect replay attack and transmits data in secure fashion

6. Future Scope

Providing protection or security on each sensor node within memory and on network messages is our action through planned work SNPDAC. Since there some practical

limitation while developing planned system. We are limiting our work for 3 nodes and not considering whole sensing network in actual real time implementation. Through use of simulation or by extending additional nodes we are able to enhance the system for big scale network wherever a lot of network transition would possibly dispense. In such case we've to focus on all network ways of whole network and storage overhead in node memory alongside alternative parameters.

7. Acknowledgment

Inspiration and guidance are invaluable in every aspect of life especially in the field of academics, which I have received from respected Head of Computer Department Prof. S. M. Shinde, our PG Coordinator Prof. M. D. Ingale and my guide Prof. H. A. Hingoliwla. I wish to express my science thanks and deep gratitude towards honorable Dr. M. G. Jadhav, Principal of JSCOE, and my Internal guide Prof. H. A. Hingoliwala, for providing me with the guidance on my dissertation work.

References

[1] Yao-Tung Tsou, Chun-Shien Lu, and Sy-Yen Kuo, "MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks" ,IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 6, JUNE 2013, page 2817 -2828.
[2] Verdone, R. Wireless Sensor Networks. In *Proceedings of the 5th European Conference*, Bologna, Italy, 2008.
[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in Proc. 2001 International Conference on Mobile Computing and Networking, pp. 189–199.
[4] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proc. 2004 International Conference on Embedded Networked Sensor Systems, pp. 162–175. \
[5] ZigBee Alliance, Zigbee specifications, Technical Report Document 053474r06, 2005.
[6] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in Proc. 2007 International Conference on Information Processing in Sensor Networks, pp. 479–488
[7] S. Kun, L. An, N. Peng, and M. Douglas, "Securing network access in wireless sensor networks," in Proc. 2009 International Conference on Wireless Network Security, pp.261–268.
[8] NIST, National Institute of Standards and Technology, Computer Security Division, AES standard. Available: http://csrc.nist.gov/archive/aes/index.html, 2001.
[9] L. Casado and P. Tsigas, "Contikisec: a secure network layer for wireless sensor networks under the Contiki operating system," in Proc. 2009 Nordic Conference on Secure IT Systems, pp. 133–147.
[10] C. M. Yu, Y. T. Tsou, C. S. Lu, and S. Y. Kuo, "Constrained function based message authentication for sensor networks," IEEE Trans. Inf. Forensic and Security, vol. 6, no. 2, pp. 407–425, 2011.

Author Profile

Mr. Uttarkar Amit is Research Scholar and PG student of Jayawantrao Sawant College of Engineering under University of Pune and currently working as Assistant professor in Computer Engineering department of JSPM NTC Pune, Maharashtra, India. He had done in Bachelors in Information Technology and having 7 years of teaching experience. His research area includes network security and Wireless sensor networks.

Prof. Hingoliwala H. A. is Associate Professor of Jayawantrao Sawant College of Engineering, Computer Department and he has having 14 years of experience. He had published more than 10 international papers and also worked as research guide for PG and UG students. He had done his Masters of Engineering from Dr. BAMU University Aurangabad, Maharashtra, India.