IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 9 (September. 2018), ||V (II) || PP 61-67

A Secure Authentication mechanism for Wireless Sensor Networks

Simran1, Maninder Kaur [2], Vijay Paul Singh [3]
M.Tech CSE student of Doaba group of colleges,affiliated by PTU university,Punjab,India
Doaba Institute of engineering &amp;Technology affiliated by PTU Jalandhar, Punjab,India
*Corresponding Author: Simran*1

Abstract— Today, wireless sensor networks are widely used due to the emergence of the Internet of Things. These networks communicate in exposed environments and as such they are susceptible to easy interception by attackers. Additionally, by its very nature, the Wireless Sensor Network environment is limited in its capacity to handle potentially sensitive information due to light security system. To provide secure and efficient mechanism, we proposed a secure authentication model in which adversary could not affect the network and genuine nodes freely communicate with each others. The proposed model introduce secure authentication through which even attacker knows the private key they could not communicate with authorized parties continuously**.**

Keywords*—**WSN; Security; Authentication; Attacks;***

Date of Submission: 31-08-2018 Date of acceptance: 15-09-2018

I. INTRODUCTION

Wireless Sensor Network is network which is deployed in an unattended environment with small sensor nodes in large number for collecting the information that is impossible for human being to reach [5]. It is very useful because they are wireless in nature and can easily gather information. Each sensor node has a capability to gather information in analog form and forward to ADC (Analog to Digital Converter) which is an internal part of sensor node, that ADC convert analog data into Digital for processing and storing. Each sensor node has four modes - transmit, receiving, sleep, idle. During transmission sensor in transmit stage and receiving sensor in receiving stage. Whereas after transmission, it goes into sleep mode to save energy and when sensor get weak due to limited power it gets into idle stage or dormant stage. During transmission data, energy consume by sensors is more than during receiving data. The main work of WSN is to gather information and that work is done by each sensor nodes which deployed in the sensor field (area where sensors are deployed). In sensor field sensor nodes are deployed with different architecture, hierarchical architecture is one of them which are very popular due to energy consumption of sensor nodes. In hierarchical there are number of routing protocol such as LEACH, PEGASIS, TEEN, APTEEN etc. , on which numbers of attack possible, In this paper we proposed a secure authentication model in which genuine nodes communicated with each others.

II. ATTACKS ON WSN

There are various threats that can affect a Wireless Sensor Network. Few of them are:

A. *Spoofed, altered, or replayed routing information:*

In this attack an attacker can create routing loops, generate false messages regarding routing updates, increase end to end delay, etc.[6]

B. *Selective forwarding:*

Some malicious nodes can delay or stop the transmission of messages by refusing to forward certain messages. In this case some messages are not propagated further. The malicious node can also behave like a black hole which rejects all the received messages. It will result in loss or drop of messages.[6]

C. *Sinkhole attacks:*

In this the attacker forces all the traffic of a specific area to pass through a compromised node.[6]

D. *Sybil attacks:*

In this a single node presents multiple identities to other nodes.[4]

E. *Wormholes:*

In this an attacker can capture messages and replays them to different nodes or in different parts by means of a tunnel.[6]

F. Replay Attack:

An attacker copies a forwarded packet and sends out the copies of the captured or intercepted traffic repeatedly and continuously to the destination node in order to exhaust the power source i.e. battery of the node , or to base stations in order to block the communication which results in degradation of network performance.

G. Denial of service attack:

The goal of this to make the network unavailable for the legitimate users. One common method of implementing this attack is to consume all the resources by sending large number of false requests so that the network is not able to provide the intended services and cannot communicate with the authenticated entities in the network [6]. The most common attack in Wireless sensor network is to flood the base station or the sink node by sending a large number of false communication requests so that it cannot communicate with registered sensor nodes which lead to the failure of tasks assigned to the network.

H. Man in Middle Attack:

The man-in-the-middle attack is a form of active attack in which the attacker establishes connections with the entities and transfer messages between them and make the entities believe that they are communicating with each other outer a private connection. The attacker will be able to intercept all messages exchanging between the two entities and also sends new
Messages.

I. Traffic Analysis Attack:

In this the attacker node attempts to examine the traffic to know the message length, communication delay, message pattern, message encoding techniques, frequency of communication etc. Traffic analysis helps in implementing other attacks which involves violation of integrity and confidentiality of messages.

J. Acknowledgement spoofing:

The goal is to convince the sender that a dead node is still alive. All the information sent to the weak links or dead node can be removed by the attacker. [6]

K. Brute Force Attack:

A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take long time to complete. A complex password can make the time for identifying the password by brute force long.[2]

III. SECURITY REQUIREMENTS IN WSN

Following are the security requirements in WSNs

• ***Availability****:* It is ensures the availability of the services offered by wireless sensor network or by a single sensor node. Resources should be available whenever required. The availability of resources can be mollified by denial of service attack [6].

• ***Authentication****:* It ensures that the entities involved in the communication are authenticated prior to the transmission of messages. The data and information should not b e available to the unauthorized no des. Only the authorized or registered no des should b e given available resources. Sensor nodes, Base station and cluster heads should b e authenticated through a proper mechanism to avoid a number of attacks possible such as impersonation attack, man in the middle attack, information theft etc. Authentication mechanism ensures that the control information or data is originated from the correct source as well as received by authenticated node [6],[7].

• ***Authorization****:*It ensures that only authorized nodes are involved in the communication[9].

• ***Integrity and freshness:***It ensures that the received message has not been changed i.e. the message must be received as it was sent by the source node. The message should be a fresh message. The sensor node or the base station must be capable of rejecting the replayed message. Adversary should not be able to forge the communication packet.

•***Confidentiality:*** It provides privacy for wireless communication channels so that the messages are not dropped or changed by an adversary. The messages exchanged between the sensor nodes or with the base station must be kept secret. The communication information must be known to the source and the destination nodes.

•***Re-authentication****:* Re Authentication must involve less communication and computational overhead than the initial authentication.

•*Untraceability:* In re-authentication of a node, source should only be able to remember the identity of the node but not direction.

•*Key Freshness:* The communicating entities should be able to verify whether the key is generated during the current session or not.

•*Node/Sink Resiliency:*If a node is compromised by an adversary it should not have any effect on the network. It is a practical threat as sensor nodes are deployed in remote areas or hostile environment.

IV. RESEARCH PAPERS

Paper I:\

Shabana et al, discuss about WSN security issues like major design challenges, security goals, threats and attacks (performance oriented, goal Oriented and Layer Oriented attacks) while collecting and processing data in Wireless Sensor Networks (WSNs) [9].

Paper II:

For Medical care Body area network consisting of small sensing and computing devices which collect various part of human body data and that data are are personal and should be private. To protect this privacy, such data are usually encrypted when transmitting it over a wireless link. One-time pads (OTPs) were mathematically proven to be secure and impossible to crack. In this paper, they present a concept for securing data transmission in BANs by utilizing OTPs. We delineate a system for generation, distribution, and utilization of OTPs in wireless sensor network (WSN) and BAN scenarios, and we show the implementation and evaluation of such a system[10].

Paper III:

Next Gen WSN generates large and different type of data. To handle such big data Hadoop is introduced to handle. As data of WSN collected in Base station. In-between Base Station and HDFS there is no security mechanism. To overcome this problem they used trust based model, through which Namenode of HDFS verify that Base Station is genuine or not. This will enhance the security of the whole mechanism and make the system secured [11].

Paper IV:

WSN condition is restricted in its ability to deal with conceivably touchy data because of light security framework. Consequently, this examination has been intended to empower the office of mysterious client verification and session enter appropriation in the transmission of touchy information all the more safely by methods for correspondence matching with sensors. It also provides user anonymity on the network so that the identity of the sender or recipient cannot be verified, and proposes a secure protocol against denial-of-service attacks and spoofing attacks [12].

Paper V:

WSN comprises of thousands of sensors and one base station. Sensors are conveyed in the system to monitor target zone and sense data as per the connected application at that point send this data to the base station. Enemy can infuse false data in the system or trade off the directing data between hubs or amongst hubs and base station. Along these lines influence the remote sensor to organize secure is viewed as a critical issue. This paper introduces an authentication protocol and simple key distributed scheme between sensor nodes. Node mobility has been taken into consideration and the work proposes a re-authentication protocol that is very efficient than the initial protocol [13].

Paper VI: This paper presents a lightweight Authentication Framework which supports node registration, entity authentication, key establishment, new node injection and broadcast authentication of messages diffusing from base towards nodes in WSN. The proposed framework is compared with other similar Schemes like Novel Access Control Protocol for secure Sensor Networks (NACP) [14].

Paper VII:

In Wireless sensor arrange security and economy of aggregate vitality are two critical and essential viewpoints; node to node verification is a vital in WSN that guarantee security. This paper propose an node to node authentication protocol with the concept of cryptography and cluster head that resolve the weakness of Diffie-Hellman key exchange scheme. The Performance of the proposed solution has been evaluated and simulated to provide a better network performance.[15]

Paper VIII:

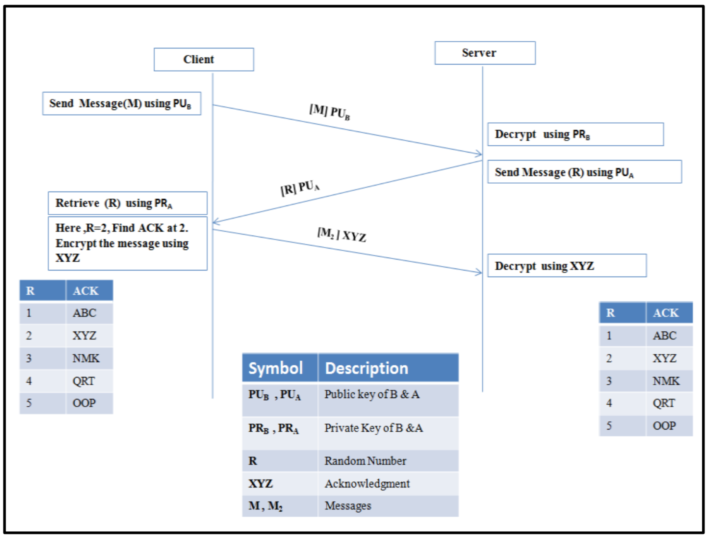
In this paper, a low overhead encryption based security solution is proposed for node authentication. The proposed node authentication scheme at the sender side consists of three modules viz. dynamic key generation, encryption and embedding of key hint [16].

Paper IX:

IoT devices quite similar to WSN or Next Gen WSN. In order to protect the WSN, a mutual authentication between devices is required during the association of a new device. The exchanged data should be authenticated and encrypted. In this they propose a robust, lightweight and energy-efficient security protocol for the WSN systems [17].

V. PROPOSED WORK

In this we consider nodes communication as a *sender receiver* or *Alice & Bob*.


Client
Server
Send Message(M) using PU_B
[M] PU_B
Decrypt using PR_B
Send Message (R) using PU_A
[R] PU_A
Retrieve (R) using PR_A
Here ,R=2, Find ACK at 2. Encrypt the message using XYZ
$[M_2]$ XYZ
Decrypt using XYZ

R	ACK
1	ABC
2	XYZ
3	NMK
4	QRT
5	OOP

Symbol	Description
PU_B , PU_A	Public key of B & A
PR_B , PR_A	Private Key of B &A
R	Random Number
XYZ	Acknowledgment
M , M_2	Messages

R	ACK
1	ABC
2	XYZ
3	NMK
4	QRT
5	OOP

We know sender and receiver both want secure communication. To perform secure communication they use encryption and decryption technique. In this way unauthorized/attacker cannot understand encrypted message, generally RSA, Diffie-Hellman etc are used for encryption and decryption.

Through Acknowledgment based authentication secure communication is possible between two authorized nodes and nodes can cross check any time. In this way man in middle attack is not possible between authorized nodes.

TABLE I.

Alice	A
Bob	B
Plain Text	M
Encryption	E
Decryption	D
Cipher text	Y, Z
Public Key of Bob	PU_B
Private Key of Bob	PR_B
Public Key of Alice	PU_A
Public Key of Alice	PR_A
Random Number	R

Step 1:- A send M to B in encrypted form using public key of B.
A—> B: Y=E [PU_{B} ,M]
Step 2:- B received A message and Decrypt it with private key PR_B
B—>A: M=D [$PR_{B,}$ Y]
Step 3:- B replied to A and Encrypt the M using public key of A.
B—>A: Z=E [PU_A , M]
Note: In this way they communicate with each other using this technique, no intruder can understand their encrypted message. If adversary "I" got private key they can easily decrypted the message and read it. To handle such type of situation we introduce this proposed algorithm.

Figure 1. Data Transfer Mechanism.

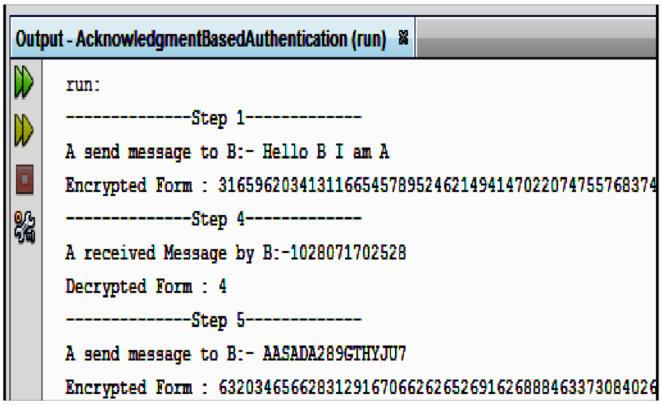
Proposed Algorithm
Step 1:- A send M to B in encrypted form using public key of B.
A —>B: Y=E [PU_{B} ,M]
Step 2:- B received A message and Decrypt it with private key PR_B
B—> A: M=D [$PR_{B,}$ Y]
Step 3:- B re-verified that A is genuine or not and send random number R to it and encrypted with public key PU_A.
B—>A: Z=E [PU_A , R]
Here, The value of R based on acknowledgment table. If somehow Attacker decrypt this, but still they can't replied to B, because they have no acknowledgment table. R lies between number of acknowledgments in acknowledgment table maintained by B.
Step 4:- A received that message and Decrypt it using PR_A and use that random number as a serial number of secure acknowledgment table and fetch value from that table ACK and encrypt the Message with that ACK and send it to B
A—> B: Q=E [ACK, M_2]
Step 5:- B received encrypt message and decrypt it with same ACK value and find A is genuine or not.
ACK=ACK
In this proposed algorithm both maintain table of acknowledgments. Whenever they communicate with each other, eventually B sends acknowledgment to the A and that acknowledgment is maintained by both for further verification. With the help of these acknowledgments they can verify each other at any moment. In the "Fig.1" the data transfer mechanism between client and server, where client communicate with server and server verifies it.

VI. IMPLEMENTATION

To simulate this we used Java programming and with the help of socket programming we perform the communication. To maintain acknowledgment table both side we use MYSQL, and to perform it we use Netbeans and implement in Window7.

Here are two cases: first case, when their communication takes place for the first time, in that case there is no need of acknowledgment verification. In second case, whenever they communicate with each other they used above proposed algorithm and they get ensured that they communicate with authorized user. Below figures shows case 2 when they re- verified each other, whenever A communicate with B , B recheck that A is genuine or not for that B use Step 3 and aftermath by receiving message from A in Step 7, where B match Acknowledgment with actual stored actual acknowledgment In this way they protect from man in middle attack.

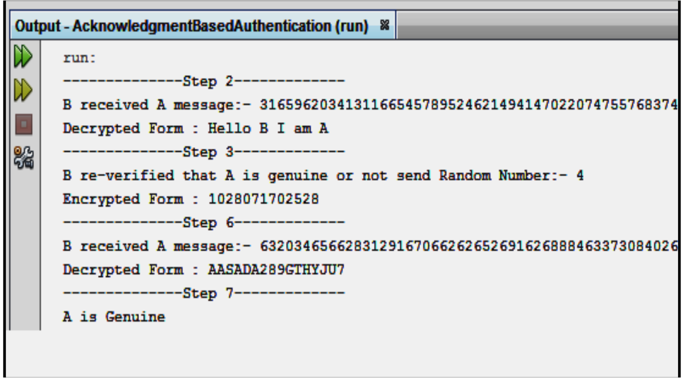
In this "Fig.2" shows the Step-1, 4, 5. of the proposed algorithm at A.



```
run:
--------------Step 1-------------
A send message to B:- Hello B I am A
Encrypted Form : 316596203413116654578952462149414702207475576837
--------------Step 4-------------
A received Message by B:-1028071702528
Decrypted Form : 4
--------------Step 5-------------
A send message to B:- AASADA289GTHYJU7
Encrypted Form : 632034656628312916706626265269162688846337308402
```

Figure 2. Node A

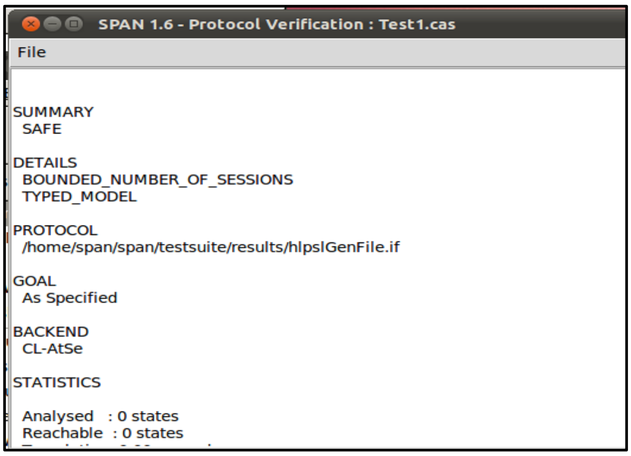
In this "Fig.3" shows the Step-2, 3, 6, 7. of the proposed algorithm at B



```
run:
--------------Step 2-------------
B received A message:- 316596203413116654578952462149414702207475576837
Decrypted Form : Hello B I am A
--------------Step 3-------------
B re-verified that A is genuine or not send Random Number:- 4
Encrypted Form : 1028071702528
--------------Step 6-------------
B received A message:- 632034656628312916706626265269162688846337308402
Decrypted Form : AASADA289GTHYJU7
--------------Step 7-------------
A is Genuine
```

Figure 3. Node B

To analysis of large-scale Internet security-sensitive protocols and applications, we used AVISPA tool [18] for the above-proposed algorithm, through this we get a SAFE result which shows, that our proposed algorithm provides secure communication between nodes



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
```

Fig : Validation results of Proposed Algorithm

VII. CONCLUSION

Security is extremely important aspect, whenever sensitive information is transferred between two nodes. There are number of security protocols which protect from attackers. WSN is collection of sensors nodes these nodes deployed on sensor field and they communicate wirelessly, Its effect that intruder can easily destroy the sensitive information or network. To proposed secure mechanism we look at various possible attacks on WSN. There are number of security protocols which protect from attackers. The above proposed algorithm verifies that users securely communicate with each other. There are number of circumstances where this proposed algorithm provides security and mitigate different attack, this algorithm secures the communication at every level and protects it from attacks by attacker.

REFERENCES

[1]. Akyildiz, Ian F., et al. "A survey on sensor networks." Communications magazine, IEEE 40.8 (2002): 102-114.

[2]. Ling, Chung-Huei, et al. "A Secure and Efficient One-time Password Authentication Scheme for WSN."*International Journal of Network Security*19.2 (2017): 177-181.

[3]. Tsuji, Takasuke, and Akihiro Shimizu. "One-time password authentication protocol against theft attacks."*IEICE transactions on communications* 87.3 (2004): 523-529.

[4]. Arampatzis, Th, John Lygeros, and Stamatis Manesis. "A survey of applications of wireless sensors and wireless sensor networks."*Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*. IEEE, 2005.

[5]. Tsudik, Gene. "Message authentication with one-way hash functions."*INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*. IEEE, 1992.

[6]. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[7]. Dogra, Heena, and Jyoti Kohli. "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey."*Indian Journal of Science and Technology* 9.47 (2016).

[8]. Lamport, Leslie. "Password authentication with insecure communication."*Communications of the ACM* 24.11 (1981): 770-772.=

[9]. SHABANA, K., FIDA, N., KHAN, F., JAN, S., REHMAN, M.. Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), North America, 5, jul. 2016.

[10]. F. Büsching and L. Wolf, "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink," in *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 63-71, Feb. 2015.

[11]. V. P. Singh, M. Hussain and C. K. Raina, "Authentication of base station by HDFS using trust based model in WSN,"*2016 International Conference on Communication and Electronics Systems (ICCES),* Coimbatore, 2016, pp. 1-5.

[12]. G. W. Choi and I. Y. Lee, "A key distribution system for user authentication using pairing-based in a WSN,"*2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, 2017, pp. 1-4.

[13]. S. S. Abd El dayem, M. R. M. Rizk and M. A. Mokhtar, "An efficient authentication protocol and key establishment in dynamic WSN,"*2016 6th International Conference on Information Communication and Management (ICICM)*, Hatfield, 2016, pp. 178-182.

[14]. A. H. Moon, U. Iqbal and G. M. Bhat, "Light weight Authentication Framework for WSN,"*2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3099-3105.

[15]. P. Joshi, M. Verma and P. R. Verma, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN,"*2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kumaracoil, 2015, pp. 527-532.

[16]. P. Banerjee, T. Chatterjee and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN,"*2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Kochi, 2015, pp. 2126-2132.

[17]. Mohamed Hammi, Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet. A Lightweight IoT Security Protocol. *1st Cyber Security in Networking Conference (CSNet2017)*, Oct 2017, Rio de Janeiro, Brazil.

[18]. Armando, Alessandro, et al. "The AVISPA tool for the automated validation of internet security protocols and applications."*International conference on computer aided verification*. Springer, Berlin, Heidelberg, 2005.

Simran1 “A Secure Authentication mechanism for Wireless Sensor Networks. ” IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 9, 2018, pp. 61-67.