Secure and Efficient Ticket based Mechanism for Mutual Authentication of Nodes in Wireless Sensor Network

[1]Pooja Gupta,[2]Chetan Kumar
[1]M.Tech Research Scholar,[2]Associate Professor
[1,2]Department of Computer Science and Engineering ,Kautilya Institute of Technology & Engineering, Jaipur, Rajasthan ,India.

Abstract : Communication is an important operation to be performed by sensor nodes carrying confidential data along with them. Hence, the security of the data is very necessary to be provided in WSN and various secure authentication mechanisms are there to ensure integrity and confidentiality of data. But most of them are not energy efficient and also have storage and communication overheads. In the proposed work, a simple, secure, energy efficient and less time-consuming protocol to provide mutual authentication of sensor nodes in WSN. This protocol is devised on the basis of tickets, where each sensor node gets a ticket from the base station(BS). The sensor nodes will then mutually authenticate each other using tickets. The base station has no role after providing tickets to the nodes. The formal analysis of the proposed protocol is done using BAN logic. The proposed protocol for authentication of sensor nodes is modeled in security analysis tool AVISPA and there are no potential attacks detected.

IndexTerms **– BAN Logic , WSN,AVISPA.**

I. INTRODUCTION

Wireless Sensor Network (WSN) can be characterized as a wireless network which comprises many distributed arrangement of sensor nodes that gather data from its encompassing condition and sensor nodes, process the data and screen them. The sensor nodes utilized in WSN speak with different nodes in wireless way. Sensor hub normally have low memory, low battery control, constrained computational capacity and low data transfer capacity. Sensor nodes are low power gadgets that straightforward calculations are performed on nearby data.

Wireless Sensor Network pursue the OSI engineering model which have five layers and three cross layers. In sensor network, there are five layers to be specific Application, Transport, Network, data Link layer and physical layer. These layers are utilized to achieve the network and make sensors cooperate. The three cross layers are Task Management plane, Mobility Management Plane and power Management plane.

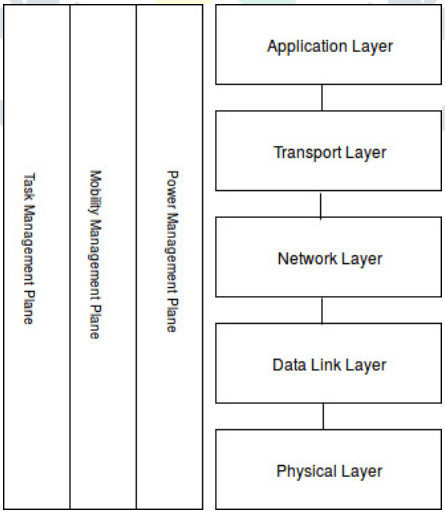


Fig 1. WSN Architecture Model[2]

WSN can be sent in condition in different ways like ad-hoc, Centralized and Distributed.

There are some real things that are viewed as significant in Security. Some security necessities are as per the following:-

Availability:- Availability characterizes that data and data of the network ought to be accessible for every one of the nodes when they required to get to them.

DoS assault influence the accessibility of the assets at any layer of network.

Confidentiality:- The Data or Information that trade between the sensor nodes or with in sensor hub and base station ought not be spilled to the gatecrashers. Classification of data give protection to correspondence channels to keep the data mystery. The personalities and open key of sensor nodes must be scrambled. Key dissemination is significant for secure correspondence between nodes.

Authentication:- It guarantees that the nodes associated with correspondence are verified before the procedure of data transmission occurred. Just approved nodes reserve the option to get to the accessible assets. There are diverse authentication component to maintain a strategic distance from assaults between the sensor nodes. An authentication component have the control that the data is started from authentication hub and gotten by validated hub

II. TYPE STYLE AND FONTS

Aneesh M.Koya and Deepthi P. P , 2018 [1] Wireless body zone networks (WBANs) assume a noteworthy job in remote wellbeing observing as a key application of the Internet of Things (IoT). Mutual authentication and key understanding are crucial for the security and protection of wellbeing data associated with the WBAN. Li et al. proposed a lightweight authentication and key understanding plan for the sensor nodes in WBAN. Their authentication and key understanding plan ensures against different existing assaults. In any case, on point by point examination, creators could find that their plan is inclined to sensor hub pantomime assault. Likewise, security of their plan depends on the supposition that the center hub is reliable, which is basically infeasible. Henceforth, creators propose a mixture unknown authentication and key understanding plan utilizing the physiological sign to beat the weaknesses in Li et al's. plot. The proposed plan likewise gives additional security highlights to oppose center point hub pantomime assault and key escrow issue. Tunnels Abadi-Needham (BAN) logic is utilized to demonstrate the rightness of the proposed plan and the Automated Validation of Internet Security Protocols and Applications (AVISPA) is utilized to assess the security of the proposed plan.

U. Jain and M. Hussain, 2017[2] Wireless sensor networks (WSN) are being utilized worldwide in numerous zones. As the application territories of the WSN are expanding at a similar rate the security dangers are likewise expanding. Interlopers are applying different components to get to the reasonable and private data from sensors. Thus, solid safety efforts are genuinely necessary to invulnerable WSNs from different assaults. Authentication is a security system that shields WSNs from wide scope of security assaults. In this paper, an authentication convention is proposed to mutually confirm sensor nodes in wireless sensor networks. The proposed convention depends on tokens. Any hub when sent in WSN is installed with base station's open key and through the comparing bunch head; it demands and procures its token for authentication from the base station. The created token is light in weight and decreases a lot of computational, communicational and capacity overheads. The proposed convention is checked for its security both officially and naturally. The proposed convention is demonstrated to be secure by assessment in BAN logic and discovered SAFE by AVISPA-a model checker apparatus for testing authentication convention.

C. Jiang, et. al 2010 [3] Wireless sensor network (WSN, Wireless Sensor Network) is a sort of independent network with sensor nodes. It is not quite the same as traditional RFID framework that the WSN is through the dispersion of sensor nodes in various areas to screen natural conditions. The gathered data from sensor nodes were sent back to the base station for further examination and preparing to repay the deficiency of traditional RFID framework. Since the WSN itself transmit messages through the wireless correspondence media, the assailant can access to make mysterious associations or hypothesis sent the message is powerless against listening in, interference and altering. It is accordingly imperative to secure the classification of data and protection for WSN network. To improve the security and protection, a proposed cover capacity is utilized to set up mutual authentication convention for WSN application. The reproduction aftereffects of the proposed mutual authentication convention are introduced. The equipment confirmation of the proposed veil capacity is exhibited on Altera DE2 demo board.

E. Yoon and K. Yoo,2011[4] Wireless sensor network (WSN) have been connected in various zones. Mutual authentication is a significant administration in WSN. In 2010, Chen and Shih proposed a powerful mutual authentication (RMA) convention for WSN. In any case, this paper calls attention to that Chen-Shih's RMA convention has a few disadvantages: (1) client pantomime assaults by a vindictive enlisted client, (2) GW-hub pantomime assaults by a malevolent enrolled client, (3) sensor hub pantomime assaults by a pernicious enlisted client, (4) advantaged insider assaults, and (5) time synchronization issue.

Xin Liu, et.al 2013[5] With wireless sensor networks (WSNs) have been connected to different fields, its security issue has turned out to be noticeable for as long as years. Subsequently it is important to structure a reasonable security authentication convention for WSNs. This paper proposes a unique mark based client authentication convention with one-time secret key for WSNs. By contrasting and other specialist's connected work, creators reach the determination that their improved convention has higher security and lower overhead execution than others.

III. PROPOSED WORK

The proposed protocol is simply elaborate by this simple diagram. This protocol is four step algorithm but considered as strong communication between nodes. It protect the nodes from different security attacks like Replay attack, Masquerade attack, Sybil attack and Dos attack. It also authenticate the nodes mutually and provide confidentiality.

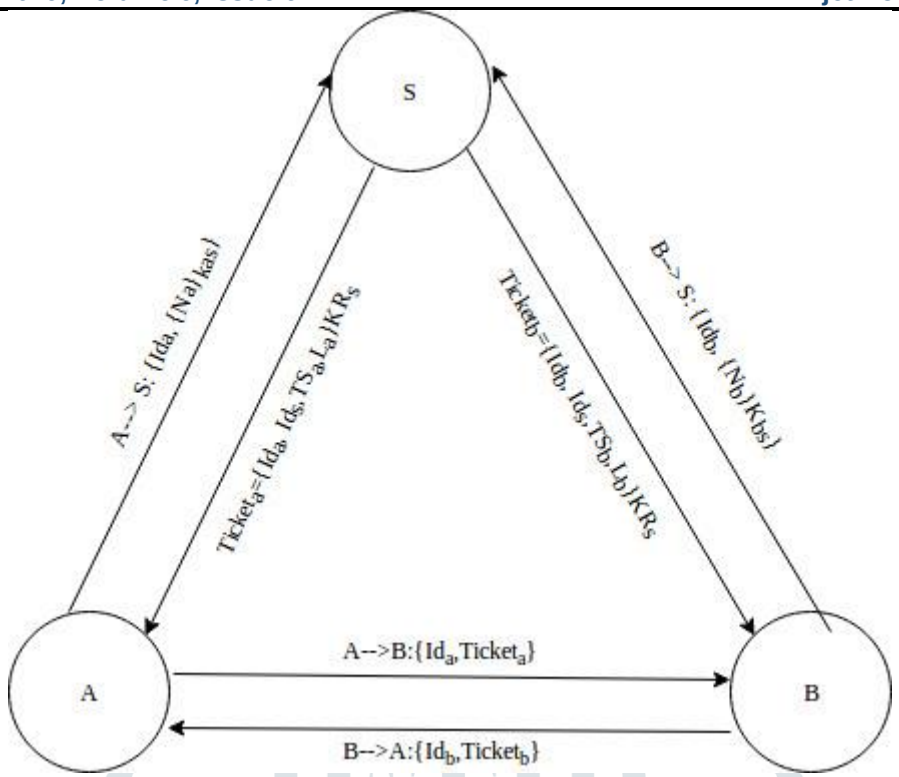


Fig 2. Diagram of proposed Protocol

This protocol is based on tickets, that is provided by ticket server(S). The proposed protocol is described here:

1: A--→S: Id_a , $\{N_a\}_{Kas}$

2: S--→A: $Ticket_a$, $\{N_a\}_{Kas}$ **Here:** $Ticket_a=\{Id_a,Id_s,TS_a,L_a\}_{KRs}$

3: B--→S: Id_b , $\{N_b\}_{Kbs}$

4: S--→ B $Ticket_b$, $\{N_b\}_{Kbs}$ $Ticket_b=\{Id_b,Id_s,TS_b, L_b\}_{KRs}$

5: A--→ B Id_a, $Ticket_a$

6: B--→ A Id_b, $Ticket_b$

The proposed scheme aims for the mutual authentication protocol for Wireless Sensor Network between the nodes using the Ticket Servers. In every sensor node of Wireless Sensor Network, Private key of Ticket Server KR_s and identity of nodes are physically stored. The Ticker Server S generate the identity and shared secret key for both nodes and private-shared key for itself. The steps of the algorithm which is used for the purpose are as follows:

Step 1: The process starts with the sensor node A wants to communicate with sensor node B. Sensor node A sends authentication request to the Ticket Server S to validate the identity.

Step 2: The Ticket Server S will validate the identity and issue the ticket.

Step 3: The other sensor node B will also request from the Ticket Server S to validate the identity.

Step 4: In the validation process the tickets for the interaction period or we can say session are issued to both nodes.

Step 5: Interaction in between the nodes will take place using the IDs of both nodes and tickets.

.

IV. Implementation and Result Analysis

4.1 AVISPA

Computerized Validation of Internet Security Protocols and Applications (AVISPA) is a push-catch apparatus for structure and examining security conventions. In this segment we present the instrument and the principals it depends on. AVISPA gives a job based, expressive formal language for convention particular and it incorporates four diverse back-closes, which per-structure the genuine investigation of the convention. We start the discourse by introducing the engineering of the apparatus and after that demonstrate the grammar of the formal language. At long last we quickly demonstrate the four back-closes that AVISPA employments.

4.2 Architecture

The engineering of AVISPA is appeared in figure 3. Initial phase in utilizing the device is to introduce the investigated convention in an extraordinary language called High Level Protocol Specification Language (HLPSL).

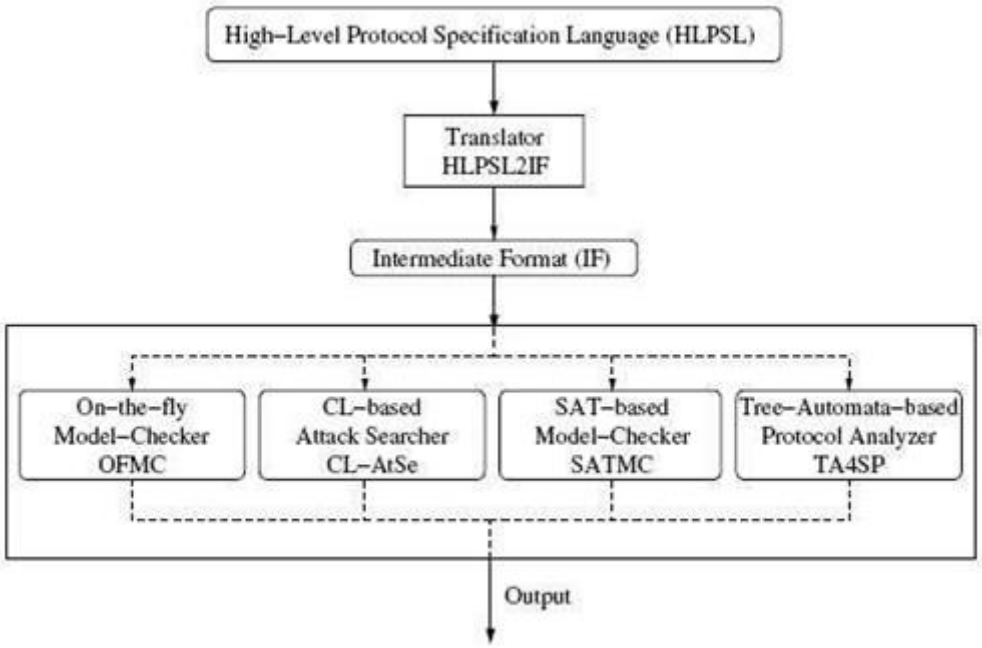


Fig 3 The architecture of the AVISPA tool .

The proposed protocol was modelled in AVISPA tool. This protocol was run in two back-end of AVISPA, OFMC and CL-AtSe. Implementation of protocol is shown and described in figures.This protocol was run in OFMC back-end of AVISPA and the result is safe.

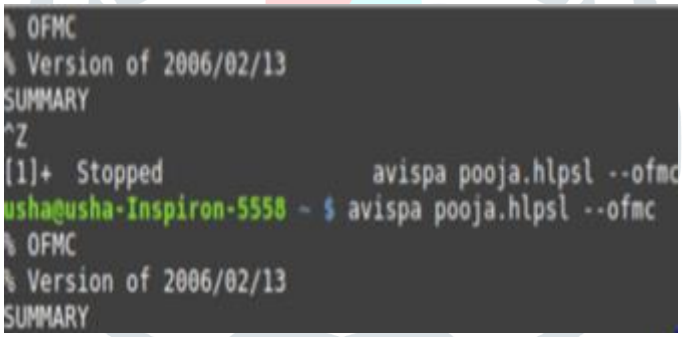
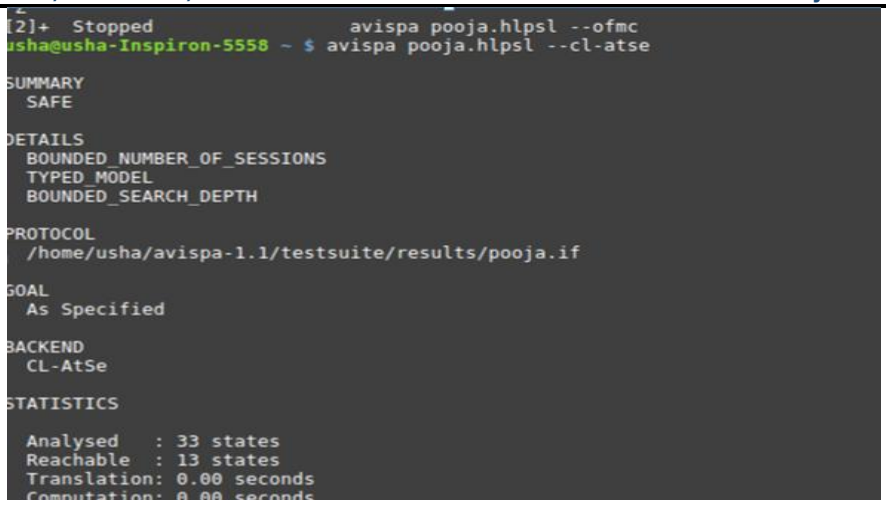


Fig 4. Simulation Results in OFMC back-end

Igure 4 shows the result of proposed protocol in OFMC back-end of AVISPA tool. OFMC back-end is On-the-Fly Model Checker defined the analysis of protocol in a demand-driven way. OFMC is used for error detection of attacks and proving the protocol correct for bounding number of sessions. The main feature of OFMC is that user can specify an algebraic theory on message terms.

It means that it is free from potential attacks. This protocol has done its execution successful when an active intruder knows the message exchanged between the agents. But intruder was unable to break or open any message and security goals are achieved by the proposed protocol i.e. authentication on Na , Nb.



.

Fig 5 Simulation Results in Cl-AtSe back-end

.This figure 5 shows the result of Cl-AtSe back-end of AVISPA tool. The Cl-AtSe (Constraint-Logic-based Attack Searcher) bases model checker transform the any security protocol specification written if IF format into set of constraints which used to find attacks on protocols. This back-end gives easily readable by anyone attacks descriptions so that they can be solved by the user easily. Our protocol result in this back-end is safe.

The result analysis of the proposed work is shown in table 1.

Table 1. Result Analysis

Aspects	**Base Paper Protocol**	**Proposed protocol**
Communication between node and cluster node	Yes	No
Communication between node and Server	No(with cluster node)	Yes
Message transmission between one to other node	less	less
Memory overhead (Nodes)	Much more	less
Cryptographic function	Asymmetric Key Hash Function	Symmetric Key encryption No Hash function
Energy Efficient	more	much more
Cost Efficient	more	much more
Computation Overhead (Nodes)	more	less

V. Conclusion

The mutual authentication between a client and a got to detecting gadget is demonstrated utilizing the broadly-acknowledged BAN logic. We have additionally demonstrated the security of the proposed plan casually and the formal security confirmation utilizing the generally acknowledged AVISPA apparatus. A thorough security examination uncovers that the proposed plan can be ensured against different known attacks by an adversary. We proposed a basic, secure, vitality productive and less tedious convention to give mutual authentication of sensor nodes in WSN. This convention depends on tickets, where every sensor hub gets a ticket from the base station(BS). The sensor nodes mutually confirm each other utilizing tickets. The base station has no job

in the wake of giving tickets to the nodes. The proposed convention for authentication of sensor nodes is demonstrated in security examination instrument AVISPA and there are no potential attacks recognized.

REFERENCES

1. AneeshM.Koya ,Deepthi P. P.,"Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", Computer Networks ,Elsevier,2018
2. U. Jain and M. Hussain, "Simple, secure and dynamic protocol for mutual authentication of nodes in wireless sensor networks," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2017, pp. 1-7.
3. C. Jiang, H. Li, Y. Huang and W. Lin, "Mutual authentication architecture in wireless sensor networks," 2010 Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia), Shanghai, 2010, pp. 291-294.
4. E. Yoon and K. Yoo, "Cryptanalysis of robust mutual authentication protocol for wireless sensor networks," IEEE 10th International Conference on Cognitive Informatics and Cognitive Computing (ICCI-CC'11), Banff, AB, 2011, pp. 392-396.
5. Xin Liu, Yongjun Shen, Shuxian Li and Fenglan Chen, "A fingerprint-based user authentication protocol with one-time password for wireless sensor networks," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Nangang, 2013, pp. 9-12.
6. H. H. Kim, N. Bruce, M. Sain, S. Park and H. Lee, "Simulation and evaluation of the authentication and session-key establishment protocol in wireless sensor networks," 2015 IEEE Conference on Wireless Sensors (ICWiSe), Melaka, 2015, pp. 7-11.
7. N. Badetia and M. Hussain, "Distributed mechanism for authentication of nodes in wireless sensor networks," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 471-474.
8. L. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," 2008 IEEE International Symposium on Wireless Communication Systems, Reykjavik, 2008, pp. 608-612.
9. H. Huang and K. Liu, "A New Dynamic Access Control in Wireless Sensor Networks," 2008 IEEE Asia-Pacific Services Computing Conference, Yilan, 2008, pp. 901-906.
10. R. Nanda, S. Tiwari and P. V. Krishna, "Secure and efficient key management scheme for wireless sensor networks," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 58-61.
11. Debiao He, N. Kumar and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, 2013, pp. 1-6.
12. Y. S. Lee, H. J. Lee and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on Physical UnclonableFunction (PUF)," 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, 2013, pp. 1314-1318.

).