JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Energy-Productive and Secure Portable Hub Reauthentication Conspire Mobile Wireless Sensor Networks

[1]Sharadhi S, [2]Nirmala M .B
[1]Student, [2]Professor
[1, 2] Department of Computer Science and Engineering,
[1, 2] Siddaganga Institute of Technology, Tumakuru, India.

Abstract: Security is a major concern on wireless network and which considered as a prioritised in order to safe the communication between static and mobile sensor nodes. WSN is a growing technology security aspects plays a vital role. Because WSN palys major role in transferring sensitive data and also in unconditional environments. The concern with the security for the data will be taken care from the beginning of the sensor design. In the exsisting system each and every mobile sensor network will have challenges with respect to security, like peer to peer network architecture , connecting without wire medium and dynamic connectivity. In this paper we mainly proposes model for the mobile wireless sensor networks with respect to security.

Index Terms: WSN, Mobile Wireless, Sensor Networks

I. INTRODUCTION

As there is a lot of improvement in the field of IoT , WSN are attracting significant attenetion in the IoT. In this WSS many sensor nodes will be there which are used to gather info from in and around of the surrounding and then sends that to the base station on in hop-multiple strategy. Mobile WSNs are new kind of technology in wireless network, here sensor nodes are mobile. If mobility is supported wi can achieve better network performance thatn the exsisting system. Many application based on MWSNs like in war field , habitat monitoring, healthcare needs the data communication to be secure and authentication is a primary step for proper and secure communication. Reauthentication technology for MWSN have been introduced for handling efficient frequent reauthentication which is based on symmetric key cryptography, which will produce easy mechanism which suits for sensor nodes.Sensor nodes are places in particular location so that they can be easily accessible by the authorized person. So that the authorized person can able record the data easily form the sensor node of MWSNs in the form of cryptographic secrets. The compromised node of mobile node will help to give the information ablout the data which is not directly involved. In our method, we tried to implement the strenght efficient reauthentication for the moving node that is called asEMSR. This mainly concentrate on satisfying the security issues and requirements by knowing the weakness and exsisting method scheme. 2 keys will be used in this one is ket derivation key and other authentication key. In whiloe uses key for pair wise key for forwarding of event unconditionally.

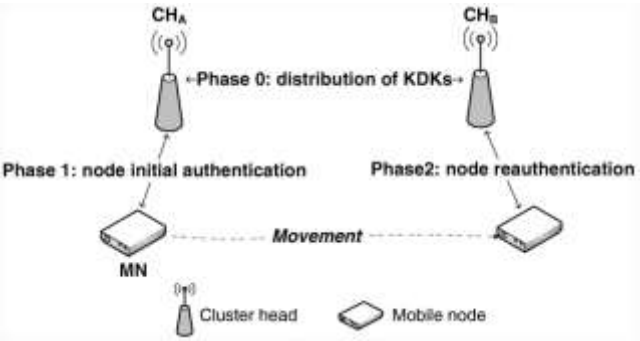

Figure 1 ***PRESENTS AN OVERVIEW OF EMSR***

II. LITRATURE SURVEY:

Moving node authentication repeatedly can be classified into two type based on condification techniques : key condification and known key condification. Later similar key condification is divided into 2 types : post-deployment and hybrid method, both uses unknown generation pre nad post distribution and deployment establishing the key mechanism.

A. Similar Key Condification Method

Haniet al. gives two ideas[9,10]. In each top pack has its own key for age ticket , this is used to ticket whichiis shared asia get-together keyiwith borderingibunchiheads. Exactly whenia compact middle factor movesito any other area and starts offevolved thezreauthentication system, the adaptable core and new gathering headZcheck eachiotheriand set up a pairwiseikey using The crucial damage of these plans is that correspondence overhead is pressed in compact middle points, thinking about the way that the bendy core factors immediately pass the records required for reauthentication,

B. Encipher Key Cyrptography Schemes

In [16], Gandino et al. proposed a affirmation and key establishment contrive difficulty to openikey cryptographyifor compact andistaticiWSNs. Inithe arrangement, approval tablesiareiusedito scale down correspondence andicomputationalioverhead as a end result of the test of mechanized support. The test tableistorei statistics primary foria core to approve a range of middle factors in the affiliation and is unfold to every core factor prior to sending. In theikeyiestablishment stage, twoicenters can verify eachiother'sipublicikeys actually usingithe approval tableias hostile to thimodernized confirmation.

III. EXSISTING_METHOD(POST DEPLOYMENT)

In this part , it has been briefly explained that what are the weakness of the security system in MWSNs and its highlights:
One of the author Han et al has been used tickets for reauthenticating the mobile node which also the security issue because all the communication was generating same authentication tokens. Each cluster head in this have capability to produce ticket(TGK) so the same will be shared with neighbour cluster heads also. In the beginning initial cluster head CHA is the one which produces the ticket T for future use of reauthentication by using its ticket generation key(for eg: TGKCHATGKCHA) . The process of producing of ticket is explained in using below equations.

$$T = (t, w)$$
$$t = E(K_{TGK_{CH_A}}, TS||R_1||K_{MN-CH_A})$$
$$w = MAC(K_{TGK_{CH_A}}, ID_{MN}||t)$$

Where_R1 is a aimless interger which is generated by moving nodeaMNiand KMN−CHAKMN−CHA , it is a known pair key within MN and CH.When MN moves to another area and takes the Hello message from the unknown top head of CHB, ,then its dispatches the reauthentication cycle:Moving node will move from one region to another while moving it takes Hello moessage from the top head of the unkown region of CHB , then it dispatches the cycle of reauthentication:

$$MN \rightarrow CH_B : ID_{MN}||ID_{CH_B}||t||w||v_1$$
$$v_1 = MAC(K_{M-CH_A}, ID_{MN}||ID_{CH_B}||t||w||v_0)$$

CHB finally creates another ticket T′, likewise that CHA did in (1) using its TGK and sends following message to MN:

$$CH_B \rightarrow MN : ID_{CH_B}||ID_{MN}||u_3||v_3$$
$$u_3 = E(K_{MN-CH_A}, R_0||v_2||T')$$
$$v_2 = H(K_{MN-CH_B}||R_0)$$
$$v_3 = MAC(K_{MN-CH_A}, ID_{CH_B}||ID_{MN}||u_3)$$

IV. PROPOSED METHOD

In the model which has been proposed, we have spirit efficient and moving node contradict method for moving nodes. ESMR is the one which will help one on one authentication and generating key within mnoving nodes and grouping heads. This is based on less consuming energy and communication for moving nodes and falls to post-deployment key generation method as shown in fugure 2.
All cluster heads have ownaKDK to produceAKs forinodes in mobile. Before networkaoperation KDK as been shared within cluster head as a common key in the group with neighbouring cluster heads. After initial authentication the cluster head at the home connectszafter zdeployment, this gives AKzforzthezmobileznodezbyzusingiKDKifor furtheriuse.
ESMR forestalls genuine sending by permitting unfamiliar group heads to validate portable hubs. Second, ESMR gives high-bargain flexibility by restricting the utilization ofztheKDKZandZAK for variousZpurposesi. Table 1 gives the significant documentations utilized in this paper.

Symbol	Description
ID_A	Identity of node A
TS_i	Timestamp
$K_{A,B}$	Pairwise key between node A and node B
KDK_A	KDK of node A
AK_A	AK of node A
$E(K,m)$	Encrypt message m with key K
$MAC(K,m)$	Message authentication code of message m with key K
||	Concatenation
$H()$	Hash function
f	Pseudorandom function
$\oplus$	Exclusive-OR operation

Table 1: Significant documentation

A. Network model

In this we think about special type of sensor community , which has baseistation , clusterihead and sensor node as proven in under discern two The cluster heads are N1 and N2 andisensor node respectively, the place n1<

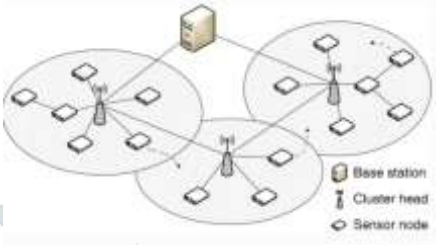

Figure 2 : Heterogenous_Sensor_Nodes

B. Adversary_model

The attack on mobile node and cluster head passively and actively. This model can easily act passive attack on wireless communication channel because of its nature. for example, snoopping and traffic investigation, to assemble data without being distinguished. In dynamic assaults, an enemy may infuse, block, or replay messages to upset organization usefulness or debase network execution.

C. Security Analysis

In this formally and imformally analysis of security of ESMR has been explained.

1. Formal verification using AVISPA

This is a tool used by many implementation of academic researchers , it will be as press button which will approve the various types of safety conventions naturally. The engineering is as displayed beneath in figure 3

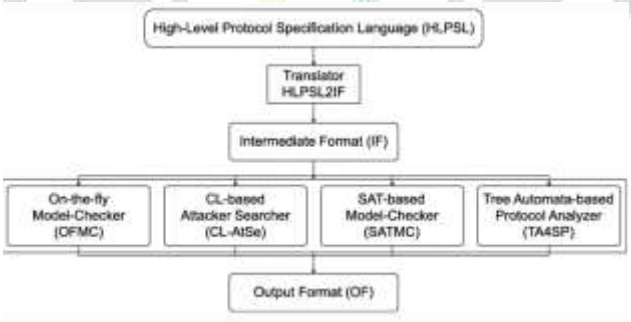

Figure 3 : AVISPA ARCHITECTURE

2. Formal Zverification Zresults

The below figure 4 shows the verification done and its results obtained in our model. For this XOR method /operationiis used. Among the four back-end tools, only OFMC and CL-AtSeisupport algebraic properties of operators such as XOR operators and exponential operators. Therefore, two back-end tools namely,iOFMC and CL-AtSe,iwere used to verify our model.

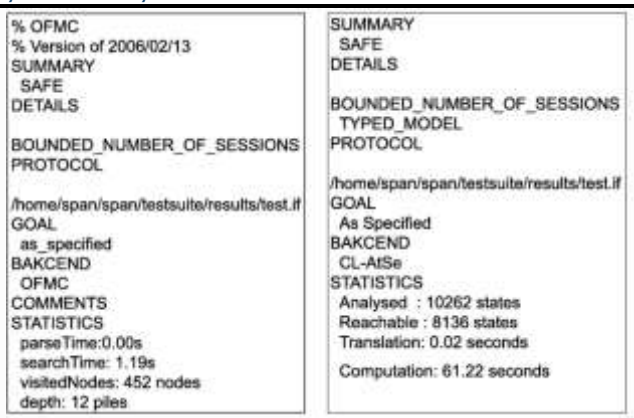

Figure 4: Verification Results

V. EVALUATION METHODOLOGY

All the three method has been checked by simulation experiemnts.

A. Energy consumption analysis result

Because all the three schemes use symmetric key cryptography, there is no significant difference in energy consumption due to computations.

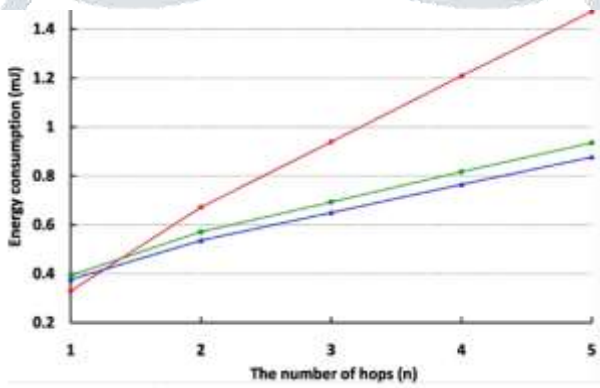

Figure 5 : For one time reauthentication total energy consumed

B. Reauthentication Latency Analysis Result

The delay based on encryption and decryption are small and which cannot be considered.

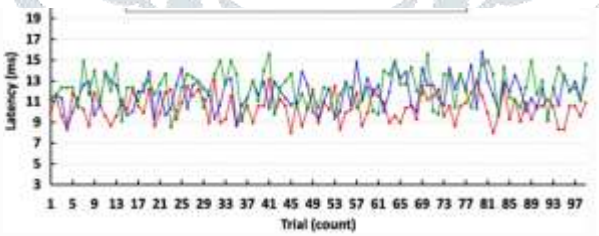

Figure 6:Reauthenticationilatencyiwheninumberiof hopsin=1

Figure 7 will give contradict latncy wrt to hops in between moving node and groupo head comparision.

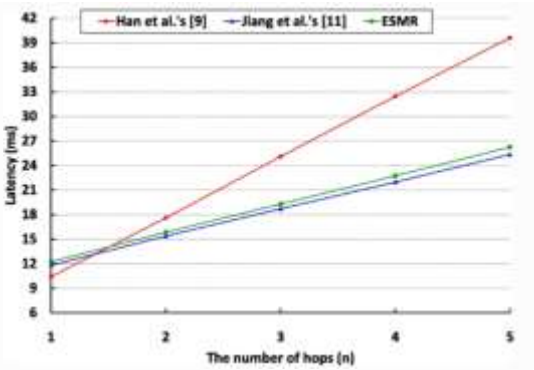

Figure 7 : Average reauthentication latency

VI. CONCLUSION

A few bendy community reauthentication plans challenge to symmetric key cryptography have been proposed to capably control predictable reauthentication Regardless, we found that Han et al's. plans don't supply high-deal adaptability and Jiang et al's. configuration experience a difficulty of real.

In this paper we have proposed confidiction-practical and ESMR for moving far off senor center point , which helps in satisfying the security essentials furthermore by considering the security. ESMR meets the security necessities of MWSNs and besides avoid security attacks.

REFERENCES

[1] X. Wang, S. Han, Y. Wu, X. Wang, Coverage and energy consumption control in mobile heterogeneous wireless sensor networks. IEEE Trans. Autom. Control.58(4), 975–988 (2020).

[2] Y. Yang, M. I. Fonoage, M. Cardei, Improving network lifetime with mobile wireless sensor networks. Comput. Commun.33(4), 409–419 (2019).

[3] O. Chipara, C. Lu, T. C. Bailey, G. -C. Roman, in Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems. SenSys ’10. Reliable clinical monitoring using wireless sensor networks: Experiences in a step-down hospital unit (ACMNew York, 2010), pp. 155–168.

[4] S. Ehsan, K. Bradford, M. Brugger, B. Hamdaoui, Y. Kovchegov, D. Johnson, M. Louhaichi, Design and analysis of delay-tolerant sensor networks for monitoring and tracking free-roaming animals. IEEE Trans. Wirel. Commun.11(3), 1220–1227 (2012).

[5] M. Li, Y. Liu, Underground coal mine monitoring with wireless sensor networks. ACM Trans. Sens. Netw. (TOSN). 5(2), 10 (2009).

[6] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, L. T. Yang, A survey on communication and data management issues in mobile sensor networks. Wirel. Commun. Mob. Com.14(1), 19–36 (2014).