Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Research Paper

A Competent Scheme For Rapid and Secure Handover Authentication Procedure of Mobile Nodes in Wireless Sensor Network

Engineering

KEYWORDS : Access point (AP), handover authentication, computation complexity, wireless sensor network (WSN), network, communication

Ms.S.Asifa Begum PG student, Nehru Institute of Technology

Mr.D.Sathish Kumar Research Scholar, Anna University, Chennai

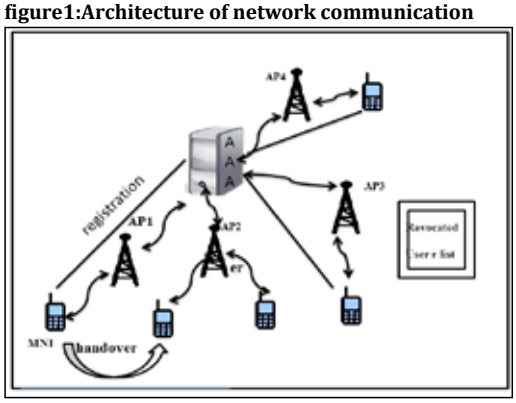
ABSTRACT

In the world of communication network it is needed to provide services to multiple users simultaneously. There is a chance of occurrence of communication delay by means of obtaining services from an increased number of access points which are formally deployed in Wireless sensor network. Security must be maintained between every handover process such as transformation of mobile nodes from one access point location to another access point location. Cryptographic key generation mechanism used For the purpose of achieving security and so computation complexity is needed to be concerned while designing the procedure of the handover authentication process of mobile users. In this paper, we proposed the scheme of an efficient handover process which resolves the essential issues like network latency by credential Ticket issuance concept and also the computation complexity is reduced with the help of reusing generated keys. The most important issue security is maintained by updating the revoked user list correspondingly by server in a network, hence authentication is done by verifying the user revocation list.

1. INTRODUCTION

Wireless sensor network is an ever growing technology which is widely used for the purpose of providing secure communication to millions of users and also it allows users to enjoy the network services effectively. The sensor nodes are used its sensing capability to monitor the weather conditions and circumstance situations. Hence, fast service Accessibility is a major thing that we need to consider to provide a solution of all participants belongs to the Network. Most of the existing approach designed for the provision of security in communication leads to complex computation. It results less concern over the speed of obtaining service while improves the authenticating process tightly to every users access. Also, it Increases the workload of the server. The main server AAA (Authentication, Accounting and Authorization) Server generates keys for a set of users' communication. All network users accessing services and involved in the process of communication only at some amount of time, once their requirement is completed as per the purpose then users get revocated from the network. It's not a predictable thing to find the number of users who joining and revocated from the network simultaneously. The server itself generates keys for the session of user communication and hence some of the generated keys become useless and wastage the memory. One of the problems with the server is its workload is higher for every authentication and verification process by every Access point, according to these problems arises in wireless sensor network (WSN). Hence the essential Issues are 1) Service delay in communication 2) provision of security throughout the communication by conducting authentication operation results the increased number of verification process with server 3) key generated for a set of users who gets revocated from the network causes the memory wastage aswellas keys become useless for any purpose . In order to solve these problems we proposed a scheme of the handover authentication process with the new procedure.

figure1:Architecture of network communication



2. RELATED WORK

Toru Nakanishi. et. Al Suggests that Revocable Group Signature Schemes with Constant Costs for Signing and Verifying with less complexity O (1). Here no need to update the secret key every time. Also, it reduces the key $\sqrt{N}$, for example the long public key of O (N) is reduced to O ($\sqrt{N}$) size public key but where signing and verification have constant extra costs.

Kai Zeng. et. al suggests the Non-Cryptographic Authentication and Identification in Wireless Networks, in this paper authentication/identification is done in 3 ways, namely software based, hardware based, channel/location based. It combines holistic, cross layer security approach using multiple layer information with traditional cryptographic mechanism. It's not an efficient scheme because cost requirement of software and hardware based authentication scheme leads to high rate of implementation.

Gianni A.et.al suggests that optimal relay node placement for throughput enhancement in wireless sensor networks, the main objective is to define relay node location for increasing the network performances by means of delivery ratio, end to end delay to provide connectivity in a partially disconnected area. It uses a dynamic routing protocol for the wireless network communication which is dynamically adapted to the changing conditions.

S. Pack. et. al suggests that fast handoff scheme that reduces the re-authentication latency in public wireless LANs. When a Mobile node sends an authentication request, the AAA server authenticates not only the currently used Access point, but also multiple Access points, and sends multiple keys to the Mobile node. These multiple APs are selected by the frequent handoff region (FHR) selection algorithm based on mobility prediction.

3. SYSTEM MODEL

3.1 Node allocation

Nodes represent the network entities which involved in the process of communication. Nodes are deployed in the wireless network Asper the functionality. Some of the nodes are act as mobile nodes (in movement) where other nodes are act as a Access point and AAA server. Initially the number of nodes required to design an architecture of network for communication is fixed. Once the node quantity is finalized then allocate the operation that needs to be performed for example server has to monitor and control the functions of all other nodes in the network, Access point has to respond the service and other requests from multiuser etc. in this way first attempt of node allocation is done and form a network for the purpose of communication.

3.2 Key Generation

Before starting the process of communication between users key generation takes the vital role for the purpose of ensuring

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

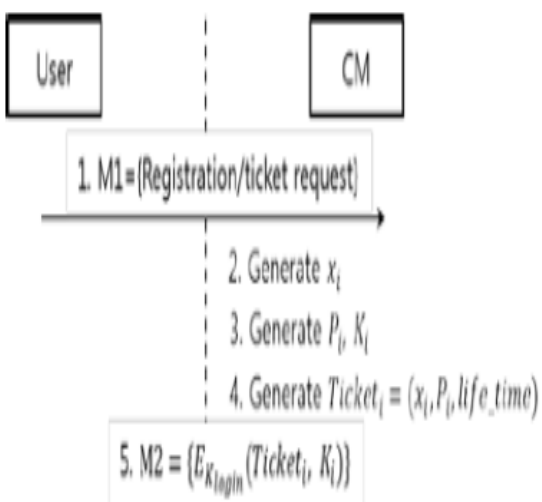
security of connected user.Initially the server generates and send master public key *mpk* to all the AP's currently involved in the networks,then each AP's share the session key AK_{AP} with AAA server respectively. also each AP has a signing/verification key pair of (sk_{AP} ,$pk_{AP)}$ the ID and pk_{AP} of each AP are publicly known to all the users.who are within the network controlled by the AP .

3.3 user registrations

Whenever the user wishes to communicate with another user in a network or getting any services from the access point, the first step is to register with AAA servers by providing the identity information of users. Only registered users are allowed to enter into a communication network process. Direct accessibility towards the access point and communication without the knowledge of a server is strictly banned here. The authorized registered user lists were sent to all Access point in a network and it must be updated frequently after every registration.

3.4 Ticket Issuance:

Once the registration is done successfully, credential ticket (C_{kj} is issued to the registered user. Tickets are generated by using the cryptographic hash function. The users are requested to start their communication process along with the ticket. It helps to server for the notification of user operation, location and its session/ expire time to participate in a network. Once the user exit from the network. Ticket become no longer usable. The user could not reenter into the network by the same ticket which is previously issued.



3.5 Handover authentication

A set of mobile nodes is transferred from one access point (AP1) to another access point (AP2) the process is called handover. Authentication needs to be done while handovering procedure carried out between AP's. First the user sends a request to the access point in order to obtain a service for communicating towards the network. Existing approaches performs this authentication operation by verifying every time with server for every request from multi users belongs to the network. it results the delay in service due to the waiting time for reply from server. So here we need to reduce the number of handshakes among involved entities. For this purpose the ticket concept is introduced. All AP's has the valid Ticket Id shared by the AAA server during the registration phase. Hence, each AP itself act as a server and Performs handover Authentication operation by itself without the involvement of server information every time. It results to improve the speed of the authentication operation handover process. Hence, communication carried out via network is very fast and secure manner.

The authentication procedure of handover process is listed below.

σ_i= G. Sign (mpk, upk_i, usk_i, rvk_i, Ω, alias|| g^{R_v} || ts, C_k)

C_i

$C_i = (alias, g^{R_v}, ts, \sigma_i)_{p^k_{AP2}}$ ⟶

Check C_k, ts, σ_i

λ_{AP2} =

ECDSA. Sig(sk_{AP2}, alias||g^{R_v}|| g^{R_v}||

K= $(g^{R_v})^{R_v}$) ⟵ g^{R_v},

λ_{AP2}

ECDSA.Ver (pk_{AP2}, $alias||g^{R_v}||g^{R_v}, \lambda_{AP2}$)

SK= $(g^{R_v})^{R_v}$ (alias|| g^{R_v}||

g^{R_v})$_{sk}$ ⟶

3.6 User Revocation list updating

AAA server maintains the user lists that are accessing the information from the server. If the user has revoked, the AAA maintains the list and updates the revoked user details. Revoked members are updated in revocation list.

If a new member is entered into the network, AAA server distributes Revocation key to the user. The revocation key is not newly generated, already used revocation key are reused.

RESULT AND ANALYSIS

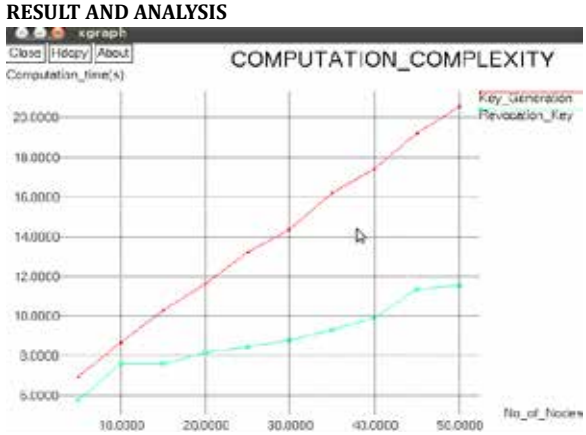


Figure 2- complexity reduction grapth

Figure2 represents how the computation complexity is reduced while using the keys of revocated users in the network communication. Hence computation time is reduced and increases the handover process as much as fast.

CONCLUSION

We analysed the characteristics of the handover process in wireless sensor network and identifies the major issues that arises between the networks in the communication. it resolves the conflicts between the security requirement and the delay in service of communication in the network. it also focuses on the computation complexity reduction of key generation. Instead of generating new keys for user it utilizes the existing keys of revocated user.it maintains the relocated user list updating concurrently for avoiding the revocated user reentry in the network. Hence we had improved the network performance metrics by means of fast handover, less computation complexity and greater security over the wireless sensor network.

REFERENCE

[1] Amit Kumar Bindal., Anuj Jain., Dr. Devendra Prasad., & Dr. R. B. Patel. (2012) Hierarchical Fault Tolerant Adaptive and Scalable Protocol for Data Dissemination in Wireless Sensor Network:HiFAS, International Journal of Applied Engineering Research, ISSN 0973-4562., 7(11). | | [2] Chin-Chen Chang. & Hao-Chuan Tsai. (2010). An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks, IEEE Trans. Wireless Comm., 9(11), 3346 - 3353. | | [3] Chun Chen, Daojing He, Sammy Chan, Jiajun Bu, Yi Gao. & Rong Fan. (2011). Lightweight and Provably Secure User Authentication with Anonymity for the Global Mobility Network, International Journal of Communication Systems, 24(3), 347-362. | | [4] Daojing He., Jiajun Bu., Chan., S. & Chun Chen. (2013). Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks , IEEE Transactions on Computers, 62(3), 616-622. | | [5] Daojing He, Maode Ma, Yan Zhang, Chun Chen. & Jiajun Bu. (2011) . A Strong User Authentication Scheme with Smart Cards for Wireless Communications, Computer Comm., 34(3), 367-374. | | [6] He, J. ,Bu S., Chan., & C. Chen (2012). Secure and efficient handover authentication based on bilinear pairing functions, IEEE Transaction of. Wireless Communication, 11(1) , 48–53. | | [7] Jaeduck Choi . & Souhwan Jung. (2010). A Handover Authentication Using Credentials Based on Chameleon Hashing, IEEE Comm. Letters, 14(1), 54-56. | | [8] Pack, S. & Choi, Y. (2004). Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems, Proc. IEE Comm., 151(5), 489-495. | [9] Pietro R.D ., Mancini L. V., Soriente, A. Spognardi, & G. Tsudik. (2009). Data security in unattended wireless sensor networks, IEEE Trans.Computers ,58(11) , 1500–1511. | | [10] Zeng.K.., Govindan k., & Mohapatra. (2010) Non-Cryptographic Authentication and Identification in Wireless Networks, IEEE Wireless Communications, 17(5),56-62. |