ISSN:0975-9646

K.SaiAditya et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1828-1832

Transitive Trust Extended Authentication Mechanism in Wireless Sensor Networks

K.SaiAditya
Department of Information Technology
SRM University
Chennai,INDIA

C.Santwana
Department of Information Technology
SRM University
Chennai,INDIA

S.Magesh
Asst.Professor(Sr.G)
SRM University
Chennai,INDIA

Abstract **- A server in a wireless sensor network handles thousands of nodes at a time. This puts a computational burden upon the server to authenticate and check each and every node for valid credentials. Instead, we propose a scheme to have an authentication mechanism that makes use of transitive trust relationships, where each authenticated node has the capability to authenticate the new nodes.**

IndexTerms *Authentication,decentralized,transitive trust xtended,wireless sensor networks .*

I. INTRODUCTION

Wireless sensor networks are gaining increasing importance in today's networking world. Their attractiveness lies in the fact that they are easier to setup, with low cost components and with no overhead of cabling. Wireless sensor networks are comprised of two entities, a *base station* and *sensor nodes.* A sensor node acts as the *source* for the data, by sensing the physical attributes of its environment like temperature, pressure, light intensity or any other measurable quantity. A sensor node is a collection of sensor circuit, processor, battery and radio. The sensor circuit is an electronic component that performs the actual sensing of the data. The processor usually converts the analog data to a digital encoding suitable to be transferred upon the wireless link. The battery is the power source for the node and usually has a very small capacity. The radio performs the transmission of data and has a limited range to ensure the conservation of energy.

The base station acts as the *sink* for the data, as it collects aggregates and forwards the sensed data to an appropriate system across a reliable wired or wireless link.

Wireless sensor networks have seen several advancements in the near past and have been employed for a long range of applications such as,

- Environmental monitoring, such as temperature, atmospheric pressure, humidity..etc.
- Disaster handling, to detect seismic waves in earthquakes, wind speed and direction in cyclones and hurricanes, forest fire detection..etc.
- Traffic handling and management, for sensing and communicating jammed routes, calling for immediate accident care..etc.

Sensor nodes are thus situated in remote/ hostile locations where recharging the battery power frequently is out of question. So each operation performed by the node is constrained by the limited battery power. Failing to focus upon this consideration may lead to frequesnt node failures, distortion of data and inability of the entire system to serve the purpose, especially in real time applications such as disaster handling and accident location propogation.

Most networks of today use a centralized approach of having a single base station, usually on the boundary of the area covered under the sensor nodes or beyond the area of service. There are several demerits of a centralized approach, which are discussed in the succeeding sections. All there demerits have been the driving force for developing a new approach for developing a decentralized authentication mechanism that addresses several problems lying in traditional systems.

Problems with a Centralized System:

A *centralized system* is the one in which all users are authenticated by the base station alone .It shown in Fig 1.

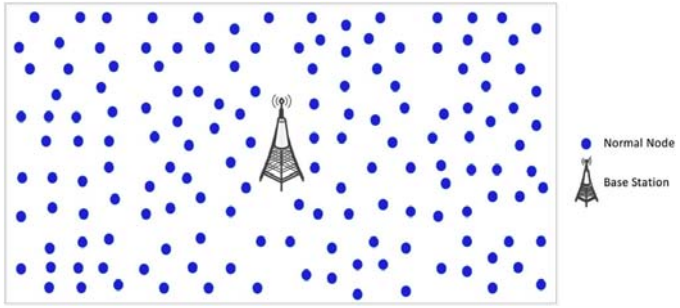


Fig 1.Basic WSN Network

An authentication scheme needs to have the following components:

1. An *authentication mechanism* to differentiate between authorized and unauthorized nodes.
2. An *access control mechanism* to ensure that the user accesses only the data that they are entitled to.
3. A *session key management scheme* that helps the secure communication of data between authenticated users. [1]

We extend these requirements for our node authentication mechanism.

A centralized scheme is easier to develop, has low setup time. Moreover, the base station has almost unlimited computational capacity, making it easier to deploy complex encryption schemes that impose high level of security. But it is not without its demerits, as discussed below:

- It makes the base station a single point of failure. A base station is the entity responsible for all computational activities and all data aggregation. Hence it becomes the target for any possible attacks from adversaries. The subversion of a base station would mean the failure of entire network in this case. [2]
- Since the communication range of the radio present in each node is short, the nodes usually employ a multi hop transmission pattern to propagate the information to the base station. This means that each node while acting as a data source for detection and sensing, also needs to act as a relay station for the data being propagated to the base station. As a result, the nodes very close to the base station deplete their power quickly because every such multi hop route needs to go through them inadvertently.
- This also makes the network susceptible to Denial of Service attack, especially upon the nodes nearer to the base station, by sending huge number of packets to run down the battery power, which could lead to a sever network failure.[1].

Hence it is suggested that a distributed approach is taken in developing the authentication scheme, so that every node of the wireless sensor network is authenticated by a local trusted node without the involvement of the base station in order to overcome the overloading of the wireless links.

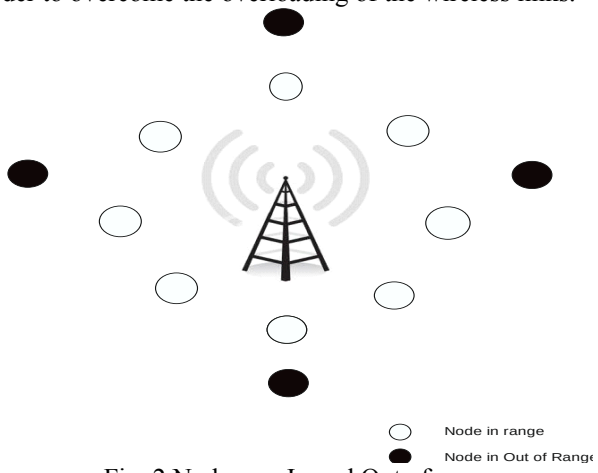


Fig 2.Nodes are In and Out of range

Security concerns of wireless sensor networks:

Since the wireless nodes often lie in unsupervised localities, they are prone to several security issues concerning the data integrity and confidentiality. Physical tampering of the nodes is also a concern to the security of the network. Poor authentication schemes may lead to introduction of spurious/malicious nodes into the network. They may distort the data being collected and obstruct the entire system from achieving its purpose.

Furthermore, with the low computational strength they have, the nodes can easily be subverted by an attacker who is equipped with higher level of computational strength.[3].

Some common types of threats in a wireless sensor network are:

Selective Forwarding attack:

This is a consequence of multi hop routing. Normally one or more nodes in the network are subverted. When sensor nodes try to forward the data to the base station, they may encounter the malicious node, which in turn replies that it has the highest quality path to the base station. All the data would then be sent through the malicious node, leading to dropping or faulty routing and in extreme cases modification of data, by damaging its integrity. This could create a black hole in the network. And usually costs high data loss to the users.[4].

Sinkhole attack:

A sinkhole attack usually forms the basis of several other attacks such as selective forwarding attack or wormhole attack. The attack may use several mechanisms for making a malicious node attractive to the other nodes, this usually happens by advertising some non verifiable properties like remaining battery power or end to end reliability. The malicious node then attracts all the data towards itself. The malicious node, depending upon its nature, may either eavesdrop the packets or modify the packets to its own advantage.[4]

Sybil Attack:

A Sybil attack is characterized by a malicious node posing as several different nodes to gain a large influence over the network. In course of time, the other nodes disjoint with one another in routing may use the same malicious node for forwarding their data. The prevention of a Sybil attack calls for unique symmetric key shared by base station with each node. [4]

There are several counter measures in order to overcome some of these attacks, such as:

1. Utilizing clustering protocols like LEACH, where cluster heads communicate with the base station on behalf of the nodes.[5]
2. Proper authentication schemes with apt cryptographic algorithms applied at each place.[5]
3. Using virtual base stations, to create an overlay network. After the virtual base stations are randomly appointed, a new multi hop topology is generated. The virtual base stations communicate directly with the real base stations. The virtual base stations are periodically changed to confuse the attackers.[4]

.**Our Proposal:**

As it is illustrated that a decentralized approach for wireless sensor networks is essential both in the efficiency as well as security point of view, we present our proposal for the authentication scheme of the wireless sensor network.

We employ **Trusted Nodes** as a part our system along with the regular nodes. These trusted nodes are similar to regular nodes in all respects except for the fact that they are ultimately trusted by the base station to authenticate the new nodes on its behalf. These trusted nodes are assumed to have a higher level of batter power compared to the normal node. It is proposed in [4] that virtual base station that change their location from time to time are an efficient defence against attackers who keep guessing the node locations. These trusted nodes can be thought of as such virtual base stations, but they are stationary and scattered all over the network domain. They share a special trust with the base station, by means of a *pre-shared key* , which is generated by the base station at the time of the trusted node registration and is updated periodically. The pre-shared key can be thought of as a nonce value generated from timestamp and other identity information of each trusted node.

The trusted nodes are then entitled to perform the authentication procedure of each and every node that is added further through a series of steps involving security operations. The security operations must always be designed with the limited computational ability of the nodes in view. High level cryptographic functions while being secure can impose additional burden on the nodes. Hence we are resorting to the operations such as XOR, which is the fastest at the hardware level and hashing, (SHA-256) which was designed with speed in mind. The idea of the authentication scheme comes from [6], which was originally developed for VANETs. Though they differ from WSNs in several respects, we consider the fact that both of them are driven by real time situations. The applications on VANETs also call for low computational complexity since they are required to produce a speedy response to any situation. Time matters in VANETs where as power matters in WSNs. The scheme that we have adopted from [6] has been cited as a low resource consuming mechanism, which justifies our use of it for WSNs.

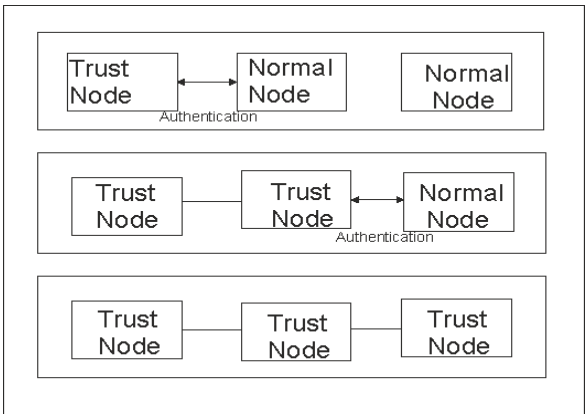


Fig 3 Transitive Trust Relationship of nodes

THE MECHANISM OF AUTHENTICATION:

We discuss the procedures for Registration, Login, Authentication, Session key establishment, Key updation procedures in the following sections.First of all, we assume that the main base station maintains the list of all the nodes under its coverage. It also has a set of keys each of which is shared apriori. These keys are called pre-shared keys and are denoted by PSK. When we mention PSK in the text, it means that it is the key related to the node in question at the base station.We denote the trusted nodes as TNodes and nodes authenticated by trusted nodes as Anodes.

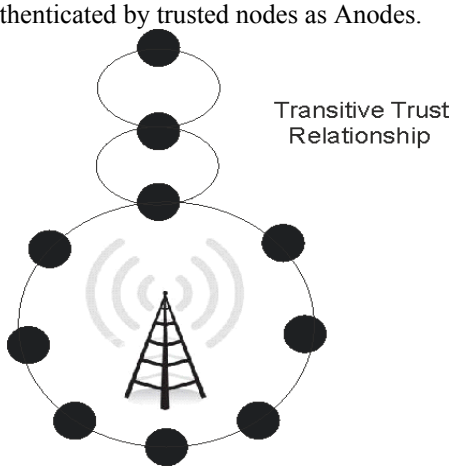


Fig 4 Nodes Authenticating Using Trust Relationship

1.TNode Registration:

The base station provides each TNode with a Preshared key value based upon a nonce. The nonce can be based upon some unique value such as the timestamp of creation of the TNode as well as the ID of the TNode. Hash functions are used to make the key values untraceable with respect to the available parameters.

2.Node Registration:

The registration of nodes happens at the time of setup. Each node has an ID and a password. But the password is not stored upon the node for security reasons. Even when adversary manages to gain the ID value from the circuit stored upon the unit, it is impossible for him to trace the password to impersonate the node, thus eliminating all possibilities of creation of fake nodes.

The parameters Ai,Bi,Ci and Di are used further in the authentication procedures. The calculation of these parameters is shown in the diagram. Ci and Bi values are essential for establishing a relationship among the ID and password values. The need for entering a password is eliminated by using Ci and Bi as can be seen in the Login procedure that follows.

LOGIN PROCEDURE:

The login procedure is the first checkpoint. The node will detect an error event immediately if the user has malicious intentions. Fig. 5 shows the steps of the login procedure.

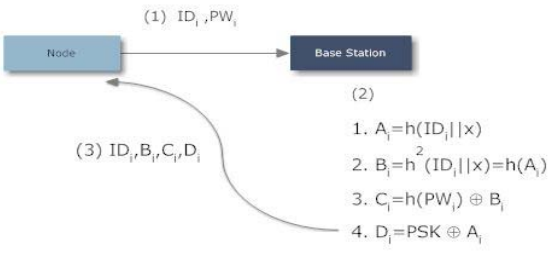


Fig 5

Step 1) $Node_i$: When a user wants to access the service, he/she inputs ID_i andPW_i to the $node_i$.

Step 2) The $Node_i$ checks the ID_i and verifies whether $h(PW_i)\oplus C_i$ is equal to B_i, where B_i and C_i are obtained from the initial registration procedure. If the information is correct, the $Node_i$ performs the general authentication procedure. Note thath$(PW_i)\oplus C_i$ has to be equal to B_i. If the values are not equal, it means that the user inputs the wrong ID_i or PW_i, resulting in the login request will be rejected.

GENERAL AUTHENTICATION PROCEDURE:

The Node performs the general authentication procedure after the user completes the login procedure. Note that the Node never uses the real identity of the user to perform the authentication procedure so nobody can obtain the Node's real identity (i.e., IDi) via the intercepted message. Fig. Shows the steps of the procedure.

Step 1) The $Node_i$ generates a random number N1 and calculates the message M1 as $h(B_i)\oplus N1$. Then, it computes the alias AID_i as $h(N_1)\oplus ID_i$, and generates the message M2 as $h(N_1||AID_i||D_i)$.

Step 2) $Node_i \rightarrow TN_j$: The $Node_i$ sends an authentication request (i.e., AID_i, M_1, M_2,D_i) to the TN_j.

Step 3) The TN_j verifies that the $Node_i$ is trustful: On receipt of the authentication request, the TN_j uses a secure preshared key (i.e., PSK) to obtain A_i (i.e., $A_i = D_i\oplus PSK$). The TN retrieves the value of N_1 (i.e., $N_1=M_1\oplus h^2(A_i)$) and then checks whether $h(N_1||AID_i||D_i)$ is equal to M_2. It rejects the authentication request if $h(N_1||AID_i||D_i)$ and M_2 do not match, which means the authentication message has been modified. Next, the TN_j computes ID_i as $AID_i\oplus h(N_1)$, generates a random number N_2, computes AID_j as $ID_j\oplus N_2$, and calculates a session key $_{SKij\ as}$ $h(N_1||N_2)$. Finally, the TN_j computes the authentication reply message (i.e., AID_j, M_3, M_4,M_5), where M_3 is $N_2\oplus h^2(N_1)$, M_4 is $A_i\oplus h(ID_i)$, and M_5 is $h(M_4||N_2||AID_j)$.

Step 4) $TN_j \rightarrow Node_i$: The TN_j returns the authentication reply message (i.e., AID_j, M_3, M_4,M_5) to the $Node_i$

Step 5) The Node verifies that the TN is trustful: The $Node_i$ computes the value of $h^2(N_1)$, retrieves the random number N_2 (i.e., $N_2=M_3\oplus h^2(N_1)$), and checks Whether $h(M_4||N_2||AID_j)$ is equal to M_5.If the information is correct, the $Node_i$ calculates the valueOf A_i(i.e.,$A_i=M_4\oplus h(ID_i)$), computes the session key(i.e., $SK_{ij}=h(N_1||N_2)$), and stores A_i in the security hardware.

Step 6) $Node_i \rightarrow TN_j$: The $Node_i$ sends the message (i.e.,SK_{ij} $\oplus h(N_2)$) to the TN_j.

Step 7) The TN uses the session key SK_{ij} to retrieve the value(i.e.,$h(N_2)$). Then, it checks this value to prevent an invalid Node from executing a replay attack.

SECURE COMMUNICATION PROCEDURE:

Two trustful nodes perform the secure communication procedure when they want to communicate with each other,as shown in Fig 6..

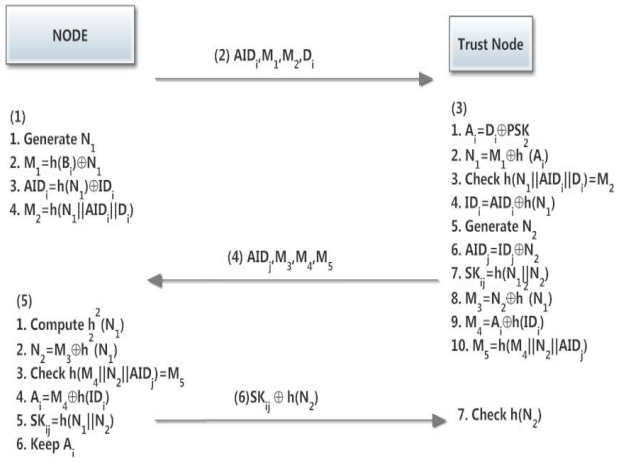


Fig 6

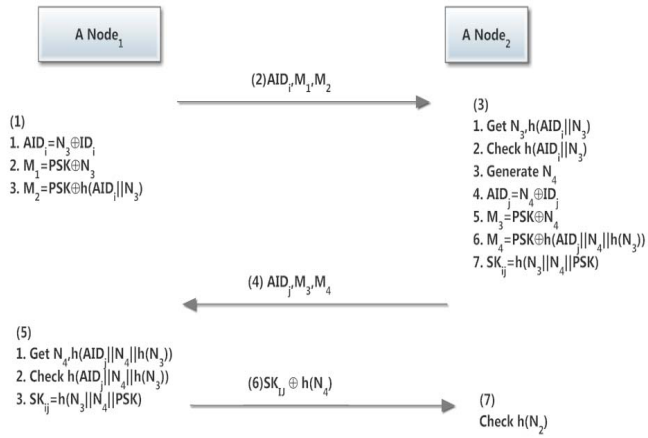
The steps are described as follows.

Step 1) After the login procedure, the $Node_i$ generates an alias AID_i and the messages for the authentication request (i.e., M_1, M_2), where N_3 is another random number, AID_i is$N_3\oplus ID_i$, M_1 is PSK$\oplus N_3$, and M2 is PSK$\oplus h(AID_i||N_3)$. Note that PSK is obtained from the general/trust-extended authentication procedure.

Step 2) $Node_i \rightarrow Node_j$: The $Node_i$ sends a secure communication request (i.e., AID_i, M_1, M_2) to the $Node_j$.

Step 3) The $Node_j$ verifies that the $Node_i$ is trustful: on receipt of the request, the Nodej uses PSK to obtain N_3 from M_1 and then checks the value of $h(AID_i||N_3)$.If the value is not correct, it means the message has been modified, and the $Node_j$ rejects the request.Next, the $Node_j$ generates a random number N_4, computes its alias AID_j, and calculates a session key SK_{ij} as $h(N_3||N_4||PSK)$. Then, the $Node_j$ computes the reply message (i.e.,M_3, M_4), where M_3 is PSK$\oplus N_4$ and M_4 is PSK$\oplus h(AID_i||N_4||h(N_3))$.

Step 4) $Node_j \rightarrow Node_i$: The $Node_j$ returns the reply message(i.e., AID_j,M_3,M_4) to the $Node_i$.



Step 5) The $Node_i$ verifies that the $Node_j$ is trustful: the $Node_i$ computes the value of $h(N_3)$, uses PSK to retrieves the random number N_4, and checks the value of $h(AID_j||N_4||h(N_3))$. If the information is correct, the $Node_i$ calculates the session key (i.e.,$SK_{ij} = h(N_3||N_4||PSK)$) for this communication.

Step 6) $Node_i \rightarrow Node_j$: the $Node_i$ sends the message (i.e.,$SK_{ij} \oplus h(N_4)$) to the $Node_j$.

Step 7) The $Node_j$ uses the session key SK_{ij} to retrieve the value (i.e.,$h(N_4)$). It then checks this value to prevent an invalid Node from executing a replay attack. Then,two trustful node can use this session key to communicate securely.

CONCLUSION

Thus we have adapted a scheme to help the authentication of wireless sensor network through a decentralized mechanism. The original paper on VANETs discusses a mechanism of using a Pre-shared key among the nodes and law executor vehicles, which we have modified as trusted nodes in our paper. The pre-shared key poses a problem in that paper as follows: Possessor of pre shared key is supposed to authenticate other vehicles, but the key update mechanism changes the pre shared key from time to time. The modified pre shared key disturbs the uniqueness of the key that is already shared among the nodes. So in our future work, we propose to develop a new mechanism for effectively distributing and updating the pre shared key without any problems of uniqueness occurring.

REFERENCES

[1] An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures, Rehana Yasmin, Eike Ritter, Guilin Wang, Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on Date June 29 2010-July 1 2010

[2] Honeybees: Combining Replication and Evasion for Mitigating Base-station Jamming in Sensor Networks, Sherif Khattab, Daniel Moss´e, and Rami Melhem, Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International Conference.

[3] Security Threats at Each Layer of Wireless Sensor Networks, Madhumita Panda, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[4] *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*, Chris Karlof and David Wagner, to appear First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003

[5] Security Threats in Wireless Sensor Networks, Sushma, Deepak Nandal, Vikas Nandal, IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011ISSN (Online): 2231 –5268

[6] TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks, Ming-Chin Chuang ; Dept. of Comput. Sci. & Inf. Eng., Nat. Chung Cheng Univ., Chiayi, Taiwan ; Jeng-Farn Lee, International Conference on Consumer Electronics, Communications and Networks (CECNet), 2011 .

[7] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards,"J. Netw. Comput. Appl., vol. 35, pp. 763–769, Mar. 2012.

[8] T. H. Chen, H. C. Hsiang, and W. K. Shih, "Security enhancement on an improvement on two remote user authentication schemes using smart cards," Future Generation Comput. Syst., vol. 27, pp. 377–380,Apr. 2011

[9] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme',"Comput. Commun., vol. 34, pp. 305–309,Mar. 2011

[10] NIST, U.S. Department of Commerce, "Secure Hash Standard," U.S.Federal Information Processing Standard (FIPS), Aug. 2002