IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-5 E-ISSN: 2347-2693

Shared Secret Key with Random Value Authentication Scheme in Wireless Sensor Networks

Madhavi Karanam

Dept. of Computer Science and Engineering,
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India

Available online at: www.ijcseonline.org

Received: Apr/26/2016 Revised: May/06/2016 Accepted: May/14/2016 Published: May/31/2016

***Abstract*—** Wireless sensor systems rearrange the gathering and investigation of information from numerous areas. Target tracking and edge interruption recognition applications are advantage from the specially appointed adhoc and self-association abilities of wireless sensor systems. Be that as it may, sensor systems conveyed in antagonistic situations must be strengthened against assaults by foes. This proposal inspects the limitations that make wireless sensor system observation testing and assesses calculations that give starting point respectability and information trustworthiness for wireless sensor systems. We propose another confirmation system. This performs superior to anything exiting strategies in terms of vitality utilization and deferral.

***Keywords*—** Authentication, Secret Key, Cryptography, Private Key, Public Key

I. INTRODUCTION

A Wireless Sensor Network (WSN) comprises of spatially disseminated self-sufficient sensors to screen physical or ecological conditions, for example, temperature, sound, vibration, weight, movement or toxins and to helpfully go their information through the system to a principle area. The more cutting edge systems are bidirectional, empowering additionally to control the action of sensors. Improvement of wireless sensor systems and its applications are available in: Military applications, for example, combat zone observation; today such systems are utilized as a part of numerous mechanical and customer applications, for example, modern procedure checking and controlling the machine, wellbeing checking, etc. A message verification code (regularly MAC) is a short bit of data used to confirm a message and to give honesty and credibility certifications on the message. Uprightness affirmations identify unplanned and deliberate message changes, while credibility guarantees and affirms the message inception. To take care of the versatility issue, a mystery polynomial based message validation plan was presented. The thought of this plan is like a limit mystery sharing, where the edge is dictated by the level of polynomial. This methodology offers data hypothetically and gives security for mutual mystery key when the quantity of messages transmitted is not exactly the limit. The middle of road hubs confirms the realness of the message through a polynomial assessment. In any case, when the quantity of messages transmitted is bigger than the limit, the polynomial can be completely recouped and the framework is totally broken.

Arrangement of wireless sensor systems in basic military and regular citizen applications requests secure confirmation. Without validation components customized to the application, sensor systems will be questionable for use in basic coliseums. The beneficiary must be ensured that basic messages undoubtedly begun from the asserted source. They should likewise have the capacity to affirm that a message was not modified in travel. Ordinary security systems being used on the Internet are typically not pertinent to wireless sensor systems on account of the constrained assets accessible in the sensor hubs, for example, restricted processor speed, littler memory size, restricted correspondence channels and speed. While security components have been proposed for wireless sensor systems, one can't aimlessly apply a security convention to a system without first comprehension the useful and security necessities of the application. Security includes some significant pitfalls; and that cost must be adjusted with objectives of the application.

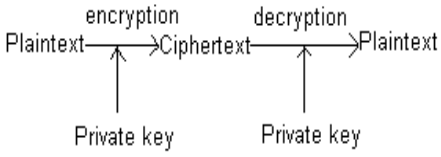

Figure 1: Cryptographic Approach

II. RELATED WORK

It is accepted that open key operation is possible for even a little sensor hub . The greater part of people in general key-based plans use a testament which is produced by BS and utilized for client verification. As a rule, be that as it may, open key operation is slower and expend considerably more

vitality than symmetric key operation. Consequently, if an aggressor dispatches DOS assault, the assailant can undoubtedly debilitate the restricted vitality of sensor node[1].

A key circulation plan for element meetings is a strategy by which at first a (disconnected from the net) trusted server conveys private individual bits of data to an arrangement of clients. Later, every individual from any gathering of clients of a given size (a dynamic meeting) can figure a typical secure gathering key. In this setting, any gathering of t clients can figure a typical key by every client processing utilizing just his private beginning bit of data and the personalities of the other t Gamma 1 clients in the gathering. Keys are secure against coalitions of up to k clients, that is, regardless of the possibility that k clients pool together their pieces they can't register anything around a key of any t-size gathering included other users [2].
This plan can give security against the replay assaults of login message and additionally acknowledge login message (Acc_login). If there should be an occurrence of login message, as GWnode checks client ID and timestamp, the foe hub can't replay it, though if there should be an occurrence of Acc_login message, as a login hub checks the authenticator, the enemy hub can't replay it. The proposed plan give common validation between login hub and passage hub. A portal hub checks the authenticator containing Ck supplied by the login hub while a login hub confirms the authenticator containing X outfitted by a passage node [3].

It gives common confirmation and session-key assertion. The plan is executed on both sides; the WSN's organizer side assuming the part of the server, and the user's device side going about as a customer. It is accept that there is an overseer, which is in charge of stacking fundamental mystery keys in the WSN and for enrollment of clients. To start with, the overseer picks a mystery key x and after that heaps the framework server and the facilitator with this mystery key x. The framework server utilizes this mystery key for enlistment of clients. The organizer utilizes this mystery key as a part of request to confirm the genuineness of clients [4].

In the TTSR (two level secure steering) plan, CHs are utilized as a spine as a part of the system so that the detected information, in the wake of being gathered, are transmitted through CHs towards the asking for clients. Between the CHs and the clients they issue SKC for confirmation. It is basically difficult to scale SKC keys to incorporate countless and sensor hubs, in light of the memory confinements. Furthermore, in SKC barring existing clients from the system and including new clients to the system, requires key disavowing and key re-dissemination, which needs a lot of correspondence overhead. These are the greatest requirements of the TTSR plan [5].

Physical altering represents a danger to sensors. In the event that sensors are circulated in an unprotected zone, an assailant could pulverize the hubs or gather the sensors, dissect the gadgets, and take cryptographic keys. This confounds the procedure of bootstrapping recently sent sensors with cryptographic keying material. To secure against this, sensors must be sealed or they should eradicate all perpetual and makeshift stockpiling when bargained. Secure key pivot components can likewise alleviate the danger of stolen cryptographic keys. Sticking assaults against wireless radio frequencies influence the accessibility of the system [6].

While it is most proficient to program sensors to convey on one particular wireless recurrence, an aggressor could without much of a stretch telecast an all the more effective sign on the same recurrence and bring obstruction into the interchanges station. Spread range advances, for example, recurrence bouncing spread range mitigate the effect of sticking; be that as it may, complex channel jumping designs decrease battery life. Hubs could likewise attempt to distinguish sticking and rest until the sticking quits, bringing about a provisional, self-affected dissent of administration (DoS) [7].

Join layer conventions confront comparatively difficult dangers. Aggressors can present crashes that compel imparting hubs to retransmit outlines. Taking after an impact, a hub must back-off and sit tight for the channel to clear before endeavoring to resend. The assailant can consistently present crashes until the casualty comes up short on force. While mistake recognizing instruments suffice for regular transmission blunders, they don't decrease the impact of malevolently produced crashes [8].

Crashes perniciously infused close to the end of a true blue casing quickly debilitate the assets of true blue hub. Confirmation can't reduce these physical and connection layer assaults. System layer assaults exploit the impromptu association of wireless sensor systems. Any hub in the system can turn into a switch, sending activity starting with one hub then onto the next. By controlling directing data, assailant can shape the stream of activity. The easiest assault bargains a directing hub and drives it to drop messages, making a system ―black hole. The aggressor can likewise specifically defer messages steered by the traded off hub. In a wormhole assault, the foe burrows messages bound for one a player in the system through a way under foe control. A wormhole assault encourages listening in, message replay, or separation of a section of the system. One procedure to make dark openings evades the way

steering conventions compose the system. Hubs ordinarily acknowledge the switch that telecasts course commercials with the most grounded radio sign [9].

This strategy diminishes the vitality required for a hub to chat with its default switch. An assailant can impact this procedure to persuade honest to goodness hubs that it requires the minimum correspondence overhead. Web style assaults have their simple in wireless sensor systems. Confusion assaults, for example, the Internet smurf assault, work in sensor systems [10].

The aggressor can drive different messages to telecast addresses with a source address manufactured to the planned casualty's location. The telecast answers will overpower the casualty, surge its correspondence station, and fumes its energy. Sifting the authentic messages from the reactions in a smurf assault needs a chain of command not display in numerous wireless sensor system steering conventions. An assault, called a Sybil assault, objects frameworks that pick peers in light of their notoriety [11].

In a Sybil assault, the enemy sends countless messages which are developed and to be sent from different hubs. Honest to goodness hubs initiate to believe the aggressor since it appears to reasonably course activity. The true blue hubs, in the long run it will acknowledge the ill-disposed hub as their switch. Transport-layer conventions present end-to-end network between hubs. For example, sequencing which is done in the Transmission Control Protocol (TCP), improves the unwavering quality of the association. Conventions that apply sequencing may respect Denial of Service (DoS) assaults. The exemplary TCP SYN surge worries to sensor systems. A foe can surge the casualty with synchronization demands and headed the capacity for different hubs to speak with the casualty. One arrangement restrains the quantity of synchronization needs acknowledged, yet this cutoff points both enemies and partners. Customer conundrums, a more mind boggling arrangement, require the customer to build a pledge to the server before it is permitted to start a discussion. At the point when the customer opens an association, the server will answer with a riddle that the customer must split. The customer must unravel the riddle and impel the response to the server before the server will perceive a full association. While this arrangement safeguards the server from SYN surges, it might harm associates that have less computational assets than the enemy does.

III. PROPOSED APPROACH

The proposed authentication technique is mainly used in the wireless sensor network where nodes are formed in the clusters. Each cluster has a cluster head. This is unique. Two nodes in a WSN communicate along at least one path of multiple intermediary nodes, determined by a suitable routing algorithm. For now we assume that there are two nodes N1CHn and NnCHn, where N1C wants to transmit a message to Nn. We also assume that there is a communication path from N1CHn to NnCHn. Here CHn is the cluster head number. In the following, shared keys will be denoted as Ki,j for a key shared between nodes NiCHn and NjCHn .

When N1(1) wants to initiate the transmission of a message m, it selects the first two nodes of a valid communication path, N2(2) and N3(3). It is required that N2(2) is a 1-hop neighbor and N3(3) is a 2-hop neighbor of N1(1).

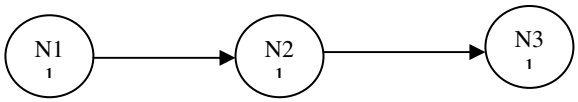

Figure 2: Message passing from N1 to N2

N1(1) creates two message authentication codes (MAC) for m using the shared keys K1,2+r and K1,3+r

a1,k = MAC((K1,k)+r, m) for k ∈ {2, 3}.

N1(1) makes sure that the origin of m is included in the body of m. That is, the identity of N1(1) is accessible through the component m.o of m. Note that this identifier is part of the original message and cannot be changed later.

N1(1) then transmits the data packet d ={m||a1,2||N3||a1,3 }to N2(2).

When a node receives a data packet, there are two cases to consider. The first case is that the data packet was just initiated by the original sender. The other case is the more general case where an inner node on the path has to forward the message towards its destination.

The next step in our example is that N2(2) receives the data packet d = {m||a1,2||N3(3)||a1,3} from N1(1).

N2(2)checks whether m.o = N1(1). N2(2) verifies that a1,2 = MAC((K1,2+r), m).

The latter step is a protection against the injection of forged messages on the link between N1(1) and N2(2). If successful, N2(2) accepts the message m.

If N2(2) accepts m and decides to forward it, N2(2) constructs new MACs a2,k = MAC((K2,k+r), m) for k ∈ {3, 4}. It then sends a new data packet d' to N3(3):

D' = {m||N1(1)||a1,3||a2,3||N4(3)||a2,4} .

In this manner all the nodes participate in message authentication technique.

IV. RESULTS

Effectiveness of proposed approach is tested by simulating random networks. Networks consist of 250 nodes, uniformly distributed on a rectangular plane (1000 m side-length), with a communication range of 100 m.

As shown in Figure3 it is observed that the proposed technique used less energy than existing technique. 'Number of Authentications' are shown in X-axis and 'Energy consumption' in the Y-axis. It is also observed that the proposed technique performs better than existing

technique in terms of delay time. In the X-axis 'Number of Authentications' and in the Y-axis 'Delay' are considered which is shown in figure4.

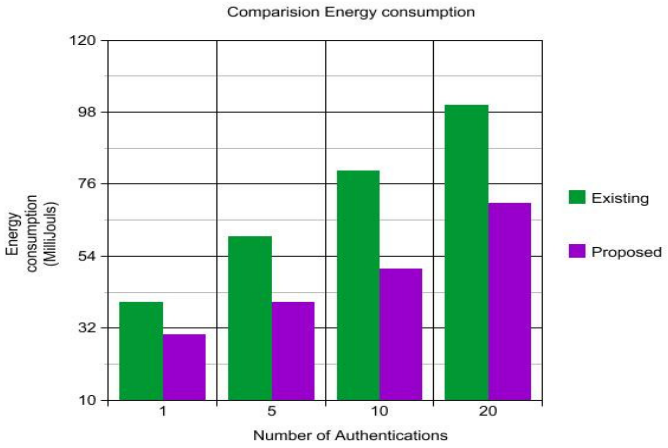

Figure 3: Energy Consumption graph

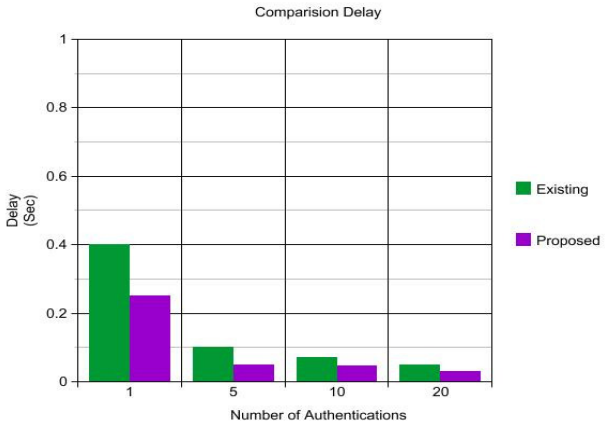

Figure 4: Delay graph

V. CONCLUSIONS

In this paper a secure and scalable user authentication scheme for wireless sensor networks is proposed to prevent intrusions. Shared key with random value used in proposed scheme is more secure. Simulation results and analysis shows that proposed scheme is not only secure and scalable than other secret key cryptography based schemes. But also requires less processing power and provides higher energy efficiency than existing public key cryptography based schemes. It is also observed that total time delay of the proposed technique is very less compare to other existing techniques.

REFERENCES

[1] Ismail Butun and Ravi Sankar." Advanced Two Tier User Authentication Scheme for Heterogeneous Wireless Sensor Networks". 2nd IEEE CCNC Research Student Workshop , 2011.

[2] Sharma S., Kumar D. (2013) "Wireless Sensor Networks- A Review on Topologies and Node Architecture". International Journal of Computer Sciences and Engineering. Vol.-1(2), pp 19-25.

[3] Binod Vaidya, Jorge Sá Silva, Joel J. P. C. Rodrigues,2009." Robust Dynamic User Authentication Scheme for Wireless Sensor Networks"proceeding of the 5th ACM symposium on QOS and security for wireless and mobile networks.

[4] Omar Cheikhrouhou1,2, Anis Koubaa3,4, Manel Boujelbenl, Mohamed Abid." A Lightweight User Authentication Scheme forWireless Sensor Networks" International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010.

[5] X. Du, G. Mohsen, X.O. Yang, C. Hsiao-Hwa. "Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks." IEEE Transactions on Wireless Communications, Vol.6 (9), pp. 3395-3401, September 2007,

[6] Panoat chuchaisri, Richard Newman,"Fast Response PKCBased Broadcast AuthenticationinWireless Sensor Networks",COLLABORATECOM 2010. DOI 10.4108/icst.collaboratecom.2010.

[7] Rasmita Rautray, Itun Sarangi(2011)," A Survey On Authentication Protocols For Wireless Sensor Network " International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462.

[8] Huei-ru Tseng, Rong-Hong Jan, Wuu Yang,"An Improved Dynamic User Authentication Scheme for WSN" NSC 94-2219-E-009-005.

[9] Er. Satish Kumar, "A Study of Wireless Sensor Networks- A Review", International Journal of Computer Sciences and Engineering, Volume-04, Issue-03, Page No (23-27), Mar -2016, E-ISSN: 2347-2693

[10] Jibi Abraham and K S Ramanatha ,"An Efficient Protocol for Authentication and Initial Shared key Establishment in clustered WSN", Proceeding of third International conference on Wireless and optical Communication networks 2006.

[11] Omar Cheikhrouhou, Anis Koubaa, Manel Boujelbenl, Mohamed Abid 2010," A lightweight user Authentication Scheme for WSN" international Conference on Sensor Networks,Ubiquitious, and Trustworthy Computing.

[12] Shamneesh Kumar, Dinesh Kumar and Keshav Kumar, " Wireless Sensor Networks – A Review on Topologies and Node Architecture", pp 19-25, Vol 1, issue 2, October, 2013.

Authors Profile

Dr.Madhavi Karanam pursed Bachelor of Engineering from Kuvenpu University,Karnataka in year 1997. She pursued M.Tech in Software Engineering form JNTUA University in 20003. She pursued Ph.D. from JNTUA University in 2013. Currently working as Professor in department of Computer Science and Engineering, GRIET, Hyderabad, INDIA. She is a life member of ISTE and CSI.She has published 15 research papers in reputed international journals and conferences including IEEE digital library and it's also available online. Her research interest includes software engineering, Model Driven Approaches, Data Mining, and Computer Networks. She has 18 years of teaching experience.