International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 11, October 2016

ISSN: 2394-4404

Enhanced Telemedicine Security Model With User Integrity Protection For Healthcare Networks

Nishu Dhiman

Chandigarh Group of Colleges

Abstract: ***The wireless sensor nodes utilizes the wireless channels in the frequency bands of the 802.11, 802.16, 802.15.4, 802.15.1 and other similar wireless standards. The wireless sensor networks are built of the small sensor nodes built upon the microcontroller platforms such as PIC, 8051, ARM, AVR, etc. During the periods when the WSN nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information. Efficient key management and distribution scheme play an important role for the data security in WSNs. Existing cryptographic key management and distribution technique usually consume higher amount of energy and put larger computational overheads on Wireless sensor nodes. The cryptographic keys are used on different communication levels of WSN communications i.e. neighbour nodes, cluster heads and base stations. A successful corporate key administration and distribution policy is required to keep up the security of the remote sensor systems. The problems described in the base papers are related to the requirement of energy efficient key exchange policies for WSNs. So to overcome the above problem there is a need to design the model to solve the key-problem of energy efficient and secure key exchange scheme. The proposed model has been found improved after the in-depth result analysis over the given scenario.***

Keywords: ***Robust authentication, Telemedicine security, Highly scrambled authentication data, Paired key based authentication.***

I. INTRODUCTION

The technological advancements in wireless communication and electronics have resulted in an exceedingly growing interest within the field of wireless detector networks. [1] A detector network involves deploying the array of sensors for distributed watching of real time events. The detector networks have restricted energy, because the detector nodes require the battery for the electronic operations. The detector nodes even have restricted memory and machine capability and might be deployed in remote areas or inhospitable piece of ground. There has been the increasing use of detector networks always important applications cherish watching patients in hospitals and military applications. These applications create it necessary to possess an honest security infrastructure for detector networks. The readying of those networks in military applications and therefore the restricted power and memory, create the look of a security protocol terribly difficult.

The security of Wireless detector Networks (WSN) will be compromised in many ways. A distant user accessing base station info will be prevented from doing thus in an exceedingly sort of ways in which. Communication between the bottom station and detector nodes will be blocked. This will be accomplished by analog attack based network jamming of signals or by digital jamming within the style of Denial of Service attacks that flood the network, base stations or each. In our own way of breaching security is to destroy the bottom station itself. This will be accomplished by watching the amount and direction of packet traffic toward the bottom station in order that the placement is eventually disclosed. Eavesdropping will be wont to track and deduce the placement of the bottom station for destruction. There are numerous alternative ways to breach the WSN security.

Several attacks are sometimes caused as a result of the shortage of security within the detector node lay communications. Parenthetically, a hacker will simply create a reference to the insecure wireless detector nodes to infect or

jam the complete detector network. These forms of attacks will be reduced or stopped by exploitation key exchange schemes that exchange the secure cryptography based scrambled keys between the nodes to make sure the safety of communications.

During the periods once the WSN nodes are in performing the operations and applications under the various conditions, they have secure cryptography based scrambled keys for secure propagation of the sensitive info. Economical key management and distribution theme play a crucial role for the information security in the sensor networks. Existing cryptography based scrambled key management and distribution technique sometimes consume higher quantity of energy and place larger machine overheads on Wireless detector Nodes. The cryptography based scrambled keys are used on completely different communication levels of WSN communications i.e. Neighboring nodes, major units as the cluster heads and base transceiver stations. An efficient company key management and distribution policy is needed to keep up the safety of the wireless detector networks. [6]

II. LITERATURE SURVEY

Ramaswamy Chandramouli et. Al. (2013) have worked on cryptography based scrambled key management problems & challenges in cloud services. The critical analysis of the common state of the application of the cryptography based scrambled operations that offer those security capabilities reveals that the management of cryptography based scrambled keys takes on an extra quality in cloud environments compared to enterprise IT environments. Ivan Damgård et. al. (2013) has projected a secure key management technique for cloud environments. Authors have studied the degree of security on the idea what they will and what they can't acquire within the security models. And when finding out that each one, authors have projected a light-weight protocols achieving peak security, and report on their sensible performance.

N. Suganthi et. Al. (2014) have projected the critical algorithmic program to support the institution of 3 styles of keys for every device node, a personal key shared with the bottom station, a combine wise key shared with neighbor device node, and a gaggle key that's shared by all the nodes within the network. The algorithmic program used for establishing and change these keys are under the energy efficient algorithm by using the smart energy consumption mechanism and minimizes the involvement of the bottom station. Zongwei Chow dynasty et. Al. (2013) has projected a brand new key management system named KISS within which the matter of fine-grained key usage management and secure system administration are resolved. Kiss aims at reducing price by hoping on hardware and minimizes the system TCB by creating the utilization of thin- hypervisor-based style and light-weight administrator devices.

Md. Monzur Morshed et. Al. (2013) have projected cluster primarily based secure routing protocol (CBSRP) may be the MANET routing protocol that ensures secure key management and communication between mobile nodes. It uses Digital Signature and a technique Hashing technique for secure communication. Consistent with CBSRP, it forms a gaggle of tiny clusters incorporates 4-5 nodes and afterward the communication takes place between mobile nodes. Marco Tiloca et. al. (2013) has projected wireless device networks ar presently utilized in several application situations, as well as industrial applications and manufactory automation. In such situations, Time Division Multiple Access (TDMA) is often used for electronic communication among device nodes. Fagen Li et. Al. (2016) projected a theme that permits a sender within the certificate-less cryptography surroundings to transmit a message to a receiver in identity primarily based cryptography surroundings .As compared with existing schemes, the machine price during this theme is reduced by concerning twenty second and fifty three .and energy consumption is reduced by concerning thirty third and fifty four. Ravi Kishore Kodali et. Al. (2014) proposes a key management technique, with its reduced resource overheads, that is extremely suited to be utilized in gradable WSN applications. Each sensor node identities primarily based key management (PBK) and probabilistic key pre-distribution schemes are created use of at completely different gradable levels. The projected key management technique has been enforced mistreatment IRIS WSN nodes.

III. DESIGN AND IMPLEMENTATION

The major problem of the cloud based platform network services lies in the security of the platform applications. The security concerns rises higher because clouds carry a higher level of exposure than the private network resources of an organization, despite of the economical or managerial benefits offered by the cloud operators. The cloud operators provide many network level security services such as firewalls, intrusion detection systems, intrusion prevention systems, various OSI model layer based security services, but lacks in the application level security services which are caused due to the application vulnerabilities or platform shortcomings. Such vulnerabilities are exposed at large due to the public access to the application resources. The hackers can easily expose the vulnerabilities of the access pages which are publically accessible and does not account for any user activity or attempt control.

The public health records are considered as the critical data. Any exposure and minor reflections in the platform record data can misguide the physicians to mention wrong prescriptions which may affect the person's health. So, it becomes very important to ensure the legitimate access to such resources. In the case of platform networks, the data is being propagated from the wireless body sensors deployed on the patient's body. Such devices can be preprogrammed for any kind of security applications while taking care of their energy constraint. The wireless body area sensors (WBAS) are the battery operated devices and must be charged almost on the daily basis. So any of the security which is being used must be energy efficient and should not reflect any effect or minor effect on the battery life of the sensor device, which ensures the longer sensing time. The longer is the sensing time of a platform body sensor, the longer becomes the monitoring periods, which always becomes beneficial for the patient health.

ISSN: 2394-4404

The proposed scheme is specially proposed for wireless platform sensor networks. The wireless user nodes are battery operated devices, Hence, having limited power sources. The platform sensors or sensor networks sends data to the platform record management services via long distance wireless communication channels such as cellular networks or radio networks. The communication between the wireless body sensor and cloud based platform service passes from many insecure network ingress or egress points, where there is higher risk of the communication data being exposed to the hackers. To protect the communication we are proposing a novel key exchange methods based upon the randomized key generation and management policy as the major improvement for the diffie-hellman scheme. Our scheme does not rely upon the key reversal or re-computational process, but is robust and rigid in nature, which does not allow any of the key guessing attacks. Such attacks do not let the sensor device to become hostile to the hackers and do not expose any information to the hackers. Our key scheme has been described in detailed below:

ALGORITHM 1: PROPOSED TELEMEDICINE BASED MULTI-LEVEL AUTHENTICATION

1. The user nodes powers up
2. The user node initiates the data propagation process
3. The user node sends data channel request to cloud platform data management server
4. The cloud platform data management server sends a verification key
5. The user node reply with the corresponding verification acknowledgement key
6. The cloud platform server verifies the authentication key my matching the authentication against the verification key
7. If key verification successful
   a. The user node is updated with an acknowledgement to send the data and start the time counter for secure channel period
8. Else
   a. The user node is denied the data connection.
9. When the secure channel period time counter expires
   a. The cloud platform server resends the verification key to the user node SN
   b. The user node reply with the corresponding verification acknowledgement key
   c. The cloud platform server verifies the authentication key my matching the authentication against the verification key
   d. If key verification successful
      i. The user node is updated with an acknowledgement to send the data and start the time counter for secure channel period
   e. Else
      i. The user node is denied the data connection.
10. Repeat the step 13 when the data communication is running

IV. RESULT ANALYSIS

The wireless network nodes are randomly deployed in the given geographic areas, which is simulated in the similar way in the proposed model simulation. The random deployments of the wireless nodes are based upon the random permutation combinations in the X and Y coordinates.

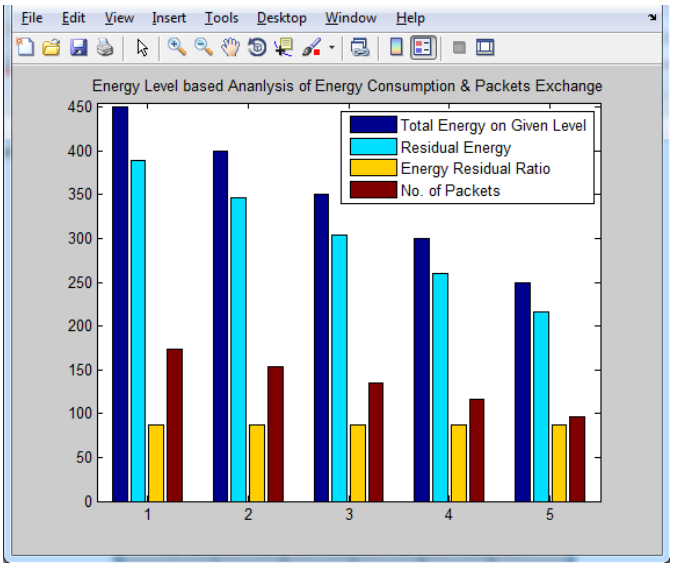

Figure 1: The energy consumption to number of packets ratio with 50 nodes

Figure 1 defines the energy consumption based variation during the different energy levels tracked in the proposed model simulation. The different energy levels have been tracked in order to understand the flow and consumption of the energy during the different packet transmission levels, which are according to the number of packets to the remaining energy ratio for the constant energy flows during the standard data transmissions. The number of the packets has been constantly decreased with the decrease in the remaining energy level to keep the similar ratio on all of the network data transmission events. In case, the energy level remains at 100 joules and the minimum energy rule over threshold set to 40 joules, each of the packet has been found consuming the 4 joules for the reception or transmission of the data. The number of packets has been found in the increasing order in the proposed model.

The time based analysis has been performed to understand the time based complexity of the proposed model during the transmission of the authentication keys. The authentication model can degrade the overall performance of the WSN networks, which becomes the reasons behind the poor network performance. In the proposed model, the time based parameters such as authentication key sharing and verification time and key generation delay. The results of the time based analysis have been defined in the depth under the scope of this section.

ISSN: 2394-4404

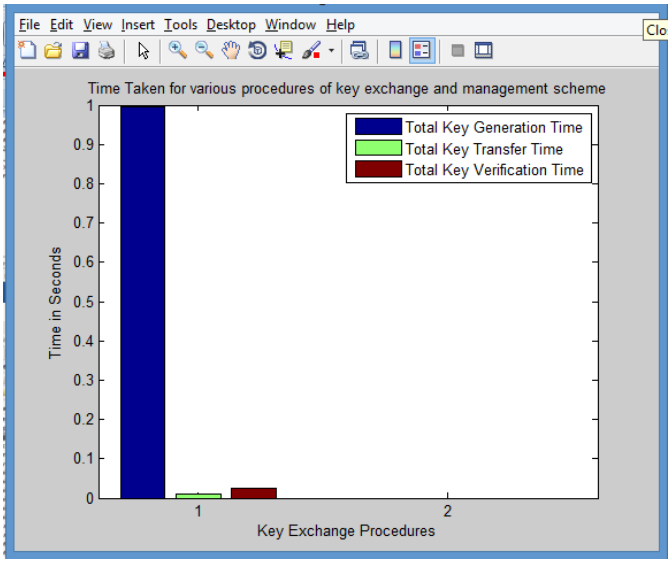

Figure 2: Elapsed time based comparative analysis

The performance of the proposed authentication scheme has been evaluated in the form of the key table generation delay, key transfer and verification delay, which also interprets the end-to-end delay for the sharing of the authentication data in the full-duplex formation. The key generation delay has been recorded nearly at 0.35 seconds, which shows the good performance by representing the optimized key table generation delay. The pair of the transmission delays (end-to-end delays), which includes the total key transfer time from the source to destination and total key verification time from destination to source nodes. The values of the key transfer and verification delay have been recorded at 0.005 seconds and 0.015 respectively. The average key verification and key transfer times are decreasing with the increase in the number of nodes, which is the result due to the availability of higher number of connections in the given sensor network topology.

V. CONCLUSION

The performance of the proposed security model for telemedicine has been also measured in the terms of the communication overhead, which has been compared to the existing model with the similar security capabilities. The proposed model has been shown the consistent trend for the communication overhead depicted in the red curve in the above figure. The proposed model has been posted the average value of nearly 0.03 KBs at almost all of the recording intervals with different number of sensor nodes, whereas the existing model has been found consistently increasing, which clearly shows the significance of the proposed model.

REFERENCES

[1] Abdallah, Walid, Noureddine Boudriga, Daehee Kim, and Sunshin An. "An efficient and scalable key management mechanism for wireless sensor networks." In *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, pp. 687-692. IEEE, 2014.

[2] Kodali, kishore Ravi. "Key management technique for WSNs." In *Region 10 Symposium, 2014 IEEE*, pp. 540-545. IEEE, 2014.

[3] Varadarajan, Prabhakar, and Garth Crosby. "Implementing IPsec in Wireless Sensor Networks." In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on*, pp. 1-5. IEEE, 2014.

[4] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.

[5] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[6] Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[7] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.

[8] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", International Conference on Emerging Technology & Factory Automation (ETFA), vol. 18, pp. 1-8, IEEE, 2013.

[9] Md. Monzur Morshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", International Advance Computing Conference (IACC), vol. 3, pp. 571-576, IEEE, 2013.