STUDIES AND REVIEWS ON ENERGY-BASED KEYING IN WIRELESS SENSOR NETWORKS

[1]V. Lokeshwari vinya, [2]V. Sreedhar, [3]Sai Sagar N, [4]Eswar Patnala
[1,3,4]Dept Of IT, GIT, GITAM University, Visakhapatnam
[2]Dept of Software Engineering, GIT, GITAM University, Visakhapatnam
[3]sagarcse539@gmail.com,[4]eswar.patnala@gmail.com

Abstract- **Now a days secure, efficient and low cost network designing becomes a challenging task in Wireless Sensor Networks (WSNs), because sensors are resource-limited wireless devices. In the present paper we analyzed and give some reviews based on the method an energy-efficient Virtual Energy-Based Encryption and Keying (VEBEK) scheme for WSNs, that significantly reduces the number of transmissions needed for rekeying to avoid stale keys which is proposed by Arif Selcuk Uluagac. In this paper various applications and protocols are discussed for optimal keying practicing. In his work RC4 algorithm is used for data encoding, which is used in the present paper to implement and support the concept of data transmission and receiving in secured communication network. In RC4 protocol a one-time dynamic key is employed for one packet only and different keys are used for the successive packets of the stream. We have evaluated VEBEK's feasibility and performance analytically and through simulations. Our results show that VEBEK, without incurring transmission overhead is able to eliminate malicious data from the network in an energy efficient manner. We implemented and analyzed the existing framework performance shows better than other comparable schemes.**

Keywords- **Wireless sensor Networks, Encryption, Decryption, dynamic keying**

I. INTRODUCTION

In the present paper a brief reviews are presented and discussed by analyzing and studying the methods proposed by Arif Selcuk Uluagac and his team [10]. We have adopted some of his concepts and methods to implement the experimental work. The simulations are carried based on the previous paper proposals. Wireless sensor networks plays major role in many of application areas. If any work has to be completed without intervention of the people , the sensors a much use full at that place. And it also reduces wired infrastructures. And the application where wired networks are used, are now replaced with the wireless sensor networks. For weather forecasting wireless sensors plays a major role because in order to receive the data from different location it impossible to use the wired infrastructure [4] because it introduces the more overhead, and if there are natural disasters like cyclones, floods, earth quakes then wired infrastructures are not the best option, at that time wireless sensors networks plays a major role, we can receive data from different centers and send the data to the centralized authority where there are monitoring all the data related to weather forecasting. When coming to another application area that is wireless sensor networks are widely used are military bases. In forest areas it is not possible to keep military forces all time in the deep thicker forest at that time wireless sensor networks came into existence, now the military forces are replaced with sensor networks. So we can know enemy movements easily [2].

In wireless sensor networks, we collect the information from the various location by spreading the sensor node to different geographic location , and the data received by the one sensor node passes that information through different intermediatary sensors nodes and reaches to the centralized authority, while travelling through the different nodes in the sensor network , the source node selects the shortest path so as to reach destination node and the node travels all the interrnediatary nodes and reach the desired centralized authority[11][12].

Now most important aspect we have discuss here about the security to the data that is traversing between the different sensor nodes because the data may be interrupted by some hackers or by some malicious code. So we have to provide the security to the data and it can be achieved by the encryption and the decryption techniques. First the data which will be ready to transmit is encrypted using some technique and the passed to different sensor nodes after it reaching to the destination node there the data will be decrypted by the centralized authority. The RC4 algorithm is used for the encryption and decryption purpose. As RC4 belongs to the symmetric cryptography same key is used for the encryption and to the decryption purpose, so it uses the shared key mechanism.

A single packet is sent along through each individual packet and hence different keys will get attached with successive packet to provide high secure network frame. Therefore, a one-time dynamic key is used for one message generated by the source sensor and different keys are used for the successive packets of the stream. The nodes are able to reduce rejections by validating the data along the path to the sink This protocol is able to continue its operations in hazardous areas where man cannot access the environments like war and under water [10][3]. VEBEK provides security services, namely authentication, integrity, and non-repudiation; thus, its flexible modular architecture allows easy adaptation for other encryption modules [10]. VEBEK's different operational modes are discussed in analytical framework [10] and a performance evaluation result including a comparison with other relevant works summarizes the design rationale and benefits of the VEBEK framework.

II. EXISTING SYSTEM

The injection of false data into WSN is detected by Dynamic Energy-based Encoding and filtering framework. Dynamic Energy-based that each sensed event report be encoded using a simple encoding scheme based on a keyed hash. The key to the hashing function dynamically changes as a function of the transient energy of the sensor, thus requiring no need for re-keying. Depending on the cost of transmission vs. computational cost of encoding, it may be important to remove data as quickly as possible. Accordingly, DEEF can provide authentication at the edge of the network or authentication inside of the sensor network [7]. Depending on the optimal configuration, as the report is forwarded, each node along the way verifies the correctness of the encoding probabilistically and drops those that are invalid. We have evaluated DEEF's feasibility and performance through analysis our results show that DEEF, without incurring transmission overhead [7].

III. REVIEW SYSTEM

The main motivation for VEBEK system to develop is for security implementation in WSN. VEBEK is a secure communication framework where sensed data is encoded using a scheme based on a permutation code generated via the RC4 encryption mechanism [10]. The key to the RC4 encryption mechanism dynamically changes as a function of the residual virtual energy of the sensor. Thus, a one-time dynamic key is employed for one packet only and different keys are used for the successive packets of the stream [10]. The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's virtual energy, thus requiring no need for specific rekeying messages. Our results show that, without increasing packet size or sending control messages for rekeying, VEBEK is able to eliminate malicious data from the network to save the energy. The encoding operation is essentially the process of permutation of the bits in the packet, according to the dynamically created permutation code via the RC4 encryption mechanism [8][9]. Since the key generation and handling process is done in another module, VEBEK's flexible architecture allows for adoption of stronger encryption mechanisms. We also show that this framework [10] performs better than other comparable schemes in the literature with an overall 60-100 percent improvement in energy savings without the assumption of a reliable medium access control layer [5][6].

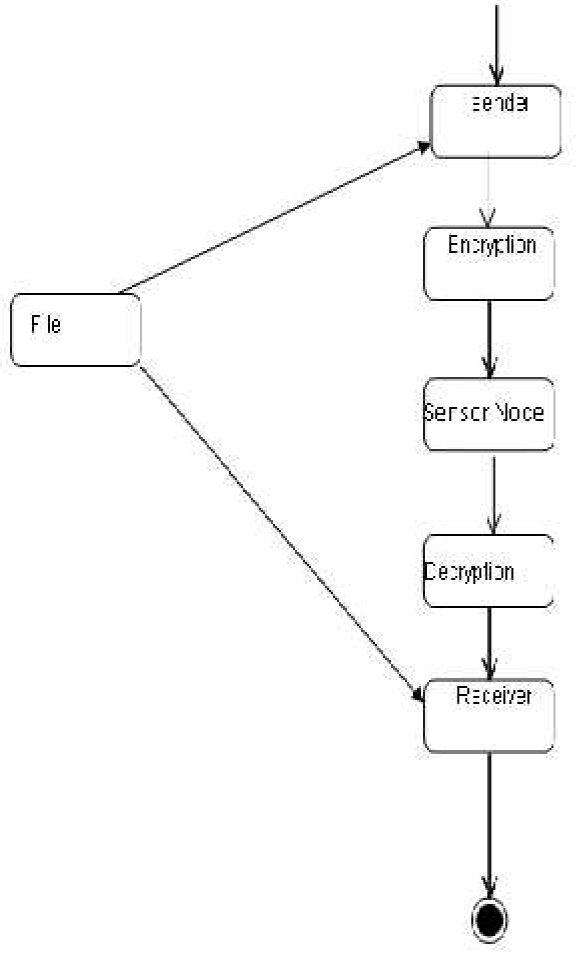

Figure 1 : State Diagram

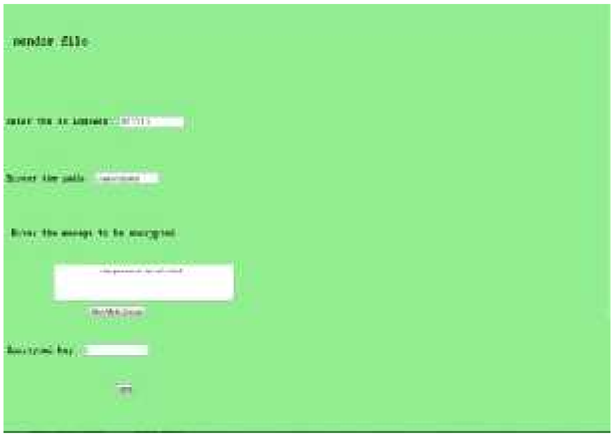

Figure 2: Enter IP Address, Select File Path, Contents of File and encrypted data

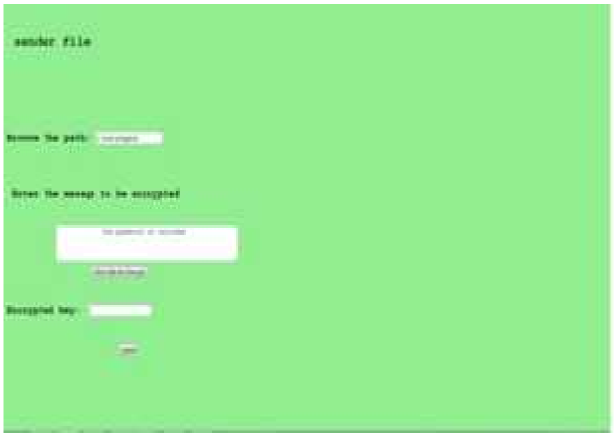

Figure 3: Sending encrypted file with encryption key

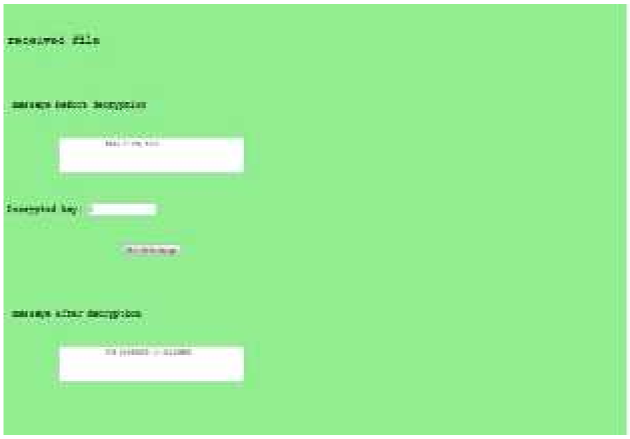

Figure 4: Receiver Receiving the encryption file and decrypt with key

We have presented some of the present experimental results which are considered from the past work. Some of the screen shots of the present work while sending the file are represented in the above diagrams. Figure 2 is showing the window contains browsing the file, entering the file content. The encrypted date is entered in the same window to encrypt the file data with the specified encrypted data. After saving the file with encrypted data send encrypted file along with encrypted key as shown in figure 3. The receiver receives the encrypted file with by decrypting the file with the help of decryption key as shown in figure 4.

IV. CONCLUSION

A secure and energy saving network is implemented based on the concerns made from a secure communication framework for WSNs called Virtual Energy- Based Encryption and Keying. In comparison with other key management schemes, we observed from the previous work done by Arif Selcuk Uluagac that, VEBEK has the following benefits: it consumes less power in key renewals by not exchange control messages. It uses one key per message to provide high security framework. The flexible modular based architecture allows easy adaptation. We have studied VEBEK's feasibility and performance through practical results and simulations by comparing with past results.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.

[2] C. Vu, R. Beyah, and Y. Li, "A Composite Event Detection in Wireless Sensor Networks," Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07), Apr. 2007.

[3] S. Uluagac, C. Lee, R. Beyah, and J. Copeland, "Designing Secure Protocols for Wireless Sensor Networks," Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008.

[4] Crossbow Technology, http://www.xbow.com, 2008.

[5] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, no. 5, pp. 51-58, 2000.

[6] R. Roman, C. Alcaraz, and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes," Mobile Networks and Applications, vol. 12, no. 4, pp. 231-244, Aug. 2007.

[7] H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.

[8] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 41-4, 2002.

[9] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic Key Management in Sensor Networks," IEEE Comm. Magazine, vol. 44, no. 4, pp. 122-130, Apr. 2006.

[10] Arif Selcuk Uluagac et al., "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks", IEEE Transactions on mobile computing, vol. 9, no. 7, july 2010.

[11] P.J.Rao, P.B.Manjeera, V.Sridevi, "Detection of rain fall and wind direction using wireless mobile sensor network", IJACMS, Bio IT journals, vol3 no3.2012 pp331-336.

[12] N. Suresh Kumar, "Design of Intelligent Multinode Sensor networking", IJCSE, Vol 2 No3, 2010, pp468-472.