Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 2 Article 4

October 2013

MAXIMIZING THE LIFETIME AND SECURITY OF WIRELESS SENSOR NETWORKS

SARANYA. S
Department of Computer Science and Engineering, G.K.M College of Engineering and Technology, Anna University, Chennai, TamilNadu, India, sarashan90@gmail.com

GOWRI. V
Department of Computer Science and Engineering, G.K.M College of Engineering and Technology, Anna University, Chennai, TamilNadu, India, gowri_vk@yahoo.co.in

Recommended Citation

S, SARANYA. and V, GOWRI. (2013) "MAXIMIZING THE LIFETIME AND SECURITY OF WIRELESS SENSOR NETWORKS," *Graduate Research in Engineering and Technology (GRET)*: Vol. 1 : Iss. 2 , Article 4.
DOI: 10.47893/GRET.2013.1022
Available at: https://www.interscience.in/gret/vol1/iss2/4

MAXIMIZING THE LIFETIME AND SECURITY OF WIRELESS SENSOR NETWORKS

SARANYA.S, GOWRI.V

Department of Computer Science and Engineering, G.K.M College of Engineering and Technology
Anna University, Chennai, TamilNadu, India
Email: sarashan90@gmail.com, gowri_vk@yahoo.co.in

Abstract—Recent technological advances have facilitated the widespread use of wireless sensor networks in many applications such as battle field surveillance, environmental observations, biological detection and industrial diagnostics. In wireless sensor networks, sensor nodes are typically power-constrained with limited lifetime, and so it’s necessary to understand however long the network sustains its networking operations. We can enhance the quality of monitoring in wireless sensor networks by increasing the WSNs lifetime. At the same time WSNs are deployed for monitoring in a range of critical domains such as military, healthcare etc. Accordingly, these WSNs are vulnerable to attacks. Now this proposed work concentrate on maximizing the security of WSNs with the already existing approach (i.e. combination of A* and fuzzy approach) for maximizing the lifetime of WSNs. This paper ensures sensed data security by providing authenticity, integrity, confidentiality. So, this approach provides more effective and efficient way for maximizing the lifetime and security of the WSNs.

I. INTRODUCTION

Wireless sensor networks (WSNs) are the foremost vital technologies which are used in variety of applications. To impact these applications in real-world environments we need more efficient strategies to guarantee security on the sensor readings as well as to prolong or maximize the network time period. WSNs use little and cheap sensor node devices; these multifunctional devices perform limited and also specific monitoring and sensing functions. The existing approach for prolonging the lifetime of WSNs is the combination of A* algorithm and Fuzzy approach for maximizing the number of connected covers [1]. The diagrammatic representation of WSNs is shown below. This paper is mainly inspired by the work in where the symmetric key (shared key) was used to ensure the protection of actual sensed data in WSNs. However, symmetric key can be extracted by an attacker through a compromised node and without checking integrity on the receiver side; this may result on delivering a modified data to a base station (BS). But now the aim of this paper is to achieve authenticity, confidentiality and integrity on the actual sensed data. For that one-way hash function and shared secret keys are used to ensure security service on the sensed data. Main objective of this paper is,

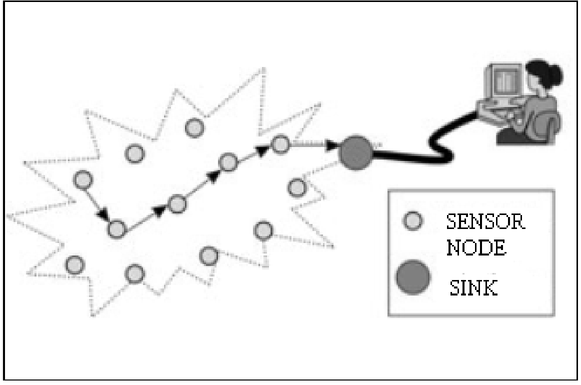

Figure 1: WSN

(1)Use the existing method A* algorithm and Fuzzy approach to find the optimal path from sensor to sink for maximizing the lifetime of WSNs.

(2) The privacy of the sensor readings will be achieved through a service of anonymity which results hiding the source node identity along the transmission path and only the base station will identify the sender.

(3) On the packet delivery along the path from source, node to base station node shared secret key and hash function will defend an attack vector, and more strong verification will be done on the receiver side (base station) to guaranty the authenticity and integrity, confidentiality of the actual sensed data. The overall architecture of the paper is shown below,

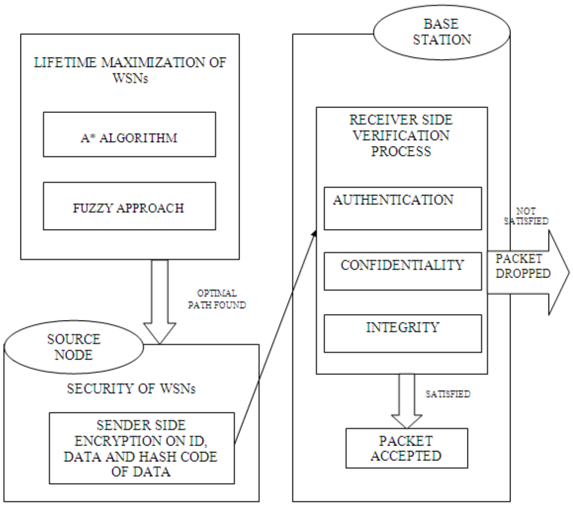

Figure 2: Overall Design

The rest of the paper is organized as follows. Section 2 Proposed work and System Architecture. In Section 3 Security analysis of proposed work. Section 4 concludes this paper.

II. PROPOSED WORK WITH SYSTEM ARCHITECTURE

This proposed security of WSNs ensures authenticity, confidentiality and integrity of the actual sensed data in WSNs by providing a checking mechanism on the receiver side. This will provide the evidence that the packet has reached the destination without being modified. Here, the first stage is to claim the liability of symmetric key, which is typically known as a single point failure based on a single shared key. Based on this, the symmetric key is also captured by en-route attack. So, data integrity checking on the receiver aspect is required through a hashing operation by ensuring that the packet received was un-altered during its transmission from a source to destination by any intermediates. Below Figure 1 is the proposed security model.

2.1. Sender Side

2.1.1. E(IDx|| Rn, Kbs).

Here, we have a tendency to apply concatenation between the source sensor ID and random number Rn(with the same size as the sensor identity) in order to provide protection against brute-force search attacks and then we encrypt them with Kbs(public Key of the base station (receiver) to provide anonymity of the source node against some attacks from attack vector.

2.1.2. E((Data), Kx,BS).

Secondly, we encrypt the sensed data with Kx,BS symmetric key shared between sender and base station (receiver), as secrecy of actual sensed data for providing confidentiality.

2.1.3. E(H(Data), Kx,BS).

Next, we apply one-way hash function on the sensed data and to enhance data security we also encrypt the message digest by the symmetric key (shared secret key between the source node and the base station). To reach the goal of ensuring authenticity , confidentiality and integrity on the sensor readings from the source to destination; then concatenate the cipher-text obtained in the previous step with the later result that becomes E(data,Kx, bs) || E(H(Data),Kx, bs).

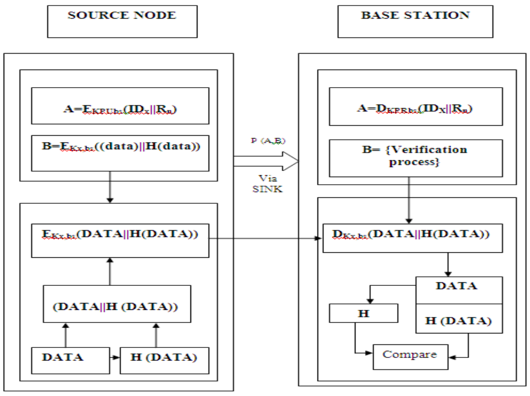
SOURCE NODE
BASE STATION
A=E_{KPUbs}(ID_x||R_n)
B=$E_{Kx,bs}$((data)||H(data))
P (A,B)
Via SINK
A=D_{KPRbs}(ID_X||R_n)
B= {Verification process}
$E_{Kx,bs}$(DATA||H(DATA))
$D_{Kx,bs}$(DATA||H(DATA))
(DATA||H (DATA))
DATA
H (DATA)
DATA
H
H (DATA)
Compare

Figure 3: Security Model

2.2. Receiver Side

2.2.1. D(IDx|| Rn,K∗BS).

Decryption to get source node identity (ID) by using the private key of the base station.

2.2.2. Integrity and Authentication Verification.

After separating the cipher text data E(Data) and the cipher text message digest E(H(Data)) both will be decrypted by using shared secret key between the source node and the base station. Next, save the plain-text message digest and then one-way hash function will be applied on the plain-text data obtained and finally we compare the result. Thus, the general method results on checking data integrity to confirm that during the transmission from the source node to destination (base station)the packet has not been modified and authenticate that the packet has been sent by legitimate user. In order to provide protection against en-route attacks from traffic analysis or fabrication during transfer from one node to another, this proposed secure communication model, which might be established with the assistance of hybrid key (asymmetric key and symmetric keyed hash function) scheme. On this basis, asymmetric key (between the sensor node and the base station) is used only for hiding the sensor node identity(anonymity), which ends up on identity privacy while the symmetric keyed hash function is used to protect the whole actual sensed data. If an adversary compromises a sensor node, he cannot with success deceive the base station to perform insider attacks, because of the infeasible computational properties of keyed hash functions. This makes it very tough for an adversary to retrieve the mandatory keys to decrypt or gain access to the original message. This conjointly provides a simple resistance within the case of nodes compromising, because the key established between non compromised nodes remains confidential.

This scheme is also resilient to the second type of node compromised, where an attacker injects the nodes within the network with the false identities. During this case, the base station will be able to detect this attack through a failure verification of our anonymity mechanism. If an insider attack (from a compromised node) gets the packet from that compromised one, it may use the last shared key to access the data, and then, the false packet can be sent with success to the base station. During this case, the false packet are composed by two concatenated contents: pretend data and real message digest. Therefore, the base station verification can indicate the attacker failure point through an authentication failure.

III. SECURITY ANALYSIS

Analyze the security of this scheme with respect to two goals: the ability of the base station to detect an altered message and the ability of the source node to mask its identity (id) for data privacy issue. In this scheme, the data packet is transmitted under the keyed hash function covered by the shared key *Kx,BS* between the sensor node and the base station. Hence, the shared key *Kx,BS* is never disclosed during transmission. The shared key *Kx,BS*is only well known by the related peers, that is, the sensor node and also the base station.

An eavesdropper at the edge of the sensor node fails to monitor or capture the random number *Rn* as well as the identity of the sensor node based on hiding features from the asymmetric key *K*bs. On this basis, without a proper matching of those dual keys (public key of the base station and private key of legitimate sensor node), any malicious node will not gain access to the context information or having the ability to forward the packets to next nodes. Therefore, this attribute may stop camouflage and traffic attacks and be helpful to shield sensor node privacy. The data packets from the sensor node to the base station are authenticated by a keyed hash function. Before accepting the inward packet data and making further processing, the receiver should verify the authentication. Based on the impossible computational properties of a hash algorithmic rule, the base station and sensor node may avoid the attacks of denial of service.

According to the above mentioned analysis, this proposed scheme, which is simple and easy to implement, can provide comparatively sturdy protection for sensor node networks.

3.1. Base Station Verification Theoretical Analysis**.**

An attacker can utilize devices with the same capabilities as the sensor nodes in the network, either by introducing sensor nodes to the networks deployment area or by destroying some of the nodes in the network under attack. Assume that an adversary *j* has known the secret key(shared) between source node and base station. *J* will have access to the concatenated data between message digest and actual sensed data. As solely base station has the knowledge of the size of the cipher text ($E[h(data),Kx,BS]$), therefore, *j* will not be able to separate the concatenated payload. If so, then the data will be stolen or only modified according to what kind of attacker, but as one-way hash function has following properties

(a) $H(x) = h$;

Where *h* equals to the result of one-way hash function of the message *x*. So given *h*, it is infeasible to find *x* (one-way

property),

(b) $H(x1) = H(x2)$ given *x*1 is infeasible to find *x*2 (weak collision resistance),

(c) $H(x1) = H(x2)$, it is infeasible to find any *x*1 and *x*2(strong collision resistance).

Therefore, the infeasible computational properties of a one-way hash function will help our scheme to identify any change that has occurred on the actual sensed data during the transmission from the source node to the base station. Thus integrity and authenticity, confidentiality will be achieved.

IV. CONCLUSION

This work proposed the security model and concatenate it with lifetime maximization technique (combination of A* algorithm and Fuzzy approach) for WSNs. Both techniques used here helped to improve the performance of the system. It achieves good level of security in terms of authenticity, integrity, and confidentiality as well as maximizing the lifetime of WSNs. This work used hybrid key technique (i.e. the combination of both symmetric and asymmetric key technique) to construct the secured communication model, unique symmetric secret key is shared between sensor node and base station which ensures the authentication, confidentiality and encrypted hashed sensed data by this key ensures integrity. Asymmetric key used to encrypt sender nodes ID which provide anonymity of the source node against some attacks from attacker. This approach overcomes the limitations caused by symmetric key encryption algorithm.

REFERENCES

[1] “Lifetime Enhancement in Wireless Sensor Networks Using Fuzzy Approach and A-Star Algorithm”, Imad S. AlShawi, Lianshan Yan, Senior Member, IEEE, Wei Pan, Member, IEEE, and Bin Luo, Member, IEEE

[2] M. Li and Y. Liu, “Rendered path: range-free localization in anisotropic sensor networks with holes,” Proceedings of the ACM MobiCom, Published in IEEE/ACM Transactions on Networking (TON), vol. 18, no. 1, pp. 320–332, 2010.

[3] M.-S. Hwang and C.-Y. Liu, “Authenticated encryption schemes: current status and key issues,” International Journal of Network Security, vol. 1, no. 2, pp. 61–Network Security, vol. 1, no. 2, pp. 61–73, 2005.

[4] Y. Ouyang, Z. Le, J. Ford, and F. Make-don, “PrivaSense: providing privacy protection for sensor networks,” The ACMConference on Embedded Networked Sensor Systems (SenSys ’07), vol. November 2007, no. Sydney, Australia.

[5] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, S. Lee, and Y. J. Song, “Achieving network level privacy in wireless sensor networks,” Sensors, vol. 10, no. 3, pp. 1447–1472, 2010.

[6] A. S. K. Pathan and C. S. Hong, “SERP: Secure energy-efficient routing protocol for densely deployed wireless sensor networks,” Annales des Telecommunications/Annals of Telecommunications, vol. 63, no. 9-10, pp. 529–541, 2008.

[7] H. C¸ am, S. O¨ zdemir, P. Nair, D. Muthuavinashiappan, and H. Ozgur Sanli, “Energy-efficient secure pattern based data aggregation for wireless sensor networks,” Computer Communications, vol. 29, no. 4, pp. 446–455, 2006.

[8] A. D. Wood, and J. A. Stankovic, “Denial of service in sensor networks,” Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[9] C. Karlof and D. Wagner, “Secure routing in sensor networks: Attacks and countermeasures,” in Proc. IEEE 1st Int. Workshop Sensor Network Protocols Applications, May 2003, pp. 113–127.

[10] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, “Two-tier secure routing protocol for heterogeneoussensor networks,” IEEE Trans.WirelessCommun.,vol. 6, no. 9, pp. 3395–3401, Sep. 2007.

[11] “A Method for Obtaining Digital Signatures and Public key Cryptosystems”, R.L. Rivest, A. Shamir, and L. Adleman MIT Laboratory for Computer Science and Department of Mathematics.

[12] “Twelve Reasons not to Route over Many Short Hops” Martin Haenggi Department of Electrical Engineering University of Notre Dame Notre Dame, IN 46556, USA.

[13] “Establishing Pairwise Keys in Distributed Sensor Networks” Donggang Liu, Peng Ning, Cyber Defense Laboratory, Department of Computer Science, North Carolina State University, Raleigh, NC 27695-8207.

◈◈◈