ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Fair Routing Across the Wireless Sensor Network Using Deniable Encryption and Load Balancing

Ashwini A N, Manjunath H R.

PG Student, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[1]

Assistant Professor, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[2]

ABSTRACT: In this paper, multiple Wireless sensor networks are not overlapped on one other and are made to communicate with each other using head nodes. In turn each wireless sensor network maintains a number of nodes within it. Each node with in a wireless sensor network contains a head node which communicates and forwards packets to the intended destination. Lifetime of each head node is maintained through the load balancing. Some malicious node is detected through the hash value of the given node. Unfortunately the malicious node, if it gets the message and decrypts it, it cannot get the original data as we us deniable encryption for providing data security. Finally, as a result there is a reduction in the energy consumption and data is secured during the transmission.

KEYWORDS: sensor network, clustering, data sealing, load balancing, fair routing

1. INTRODUCTION

In the past years, wireless sensor network has become a fast growing technology. As the name suggests, sensor networks consists of nodes called sensors. these sensors senses the data i.e., accepts the real world data and forwards the data from source to the destinations. These sensors are interconnected in a wireless fashion. There is no dedicated link between any sensor nodes. For example if there are 10 sensor nodes each sensor node is connected to remaining all sensor nodes. Generalizing if n sensor nodes are present in a network, each node is connected to n-1 nodes.

The collection or group of finite number of sensor nodes form wireless sensor nodes. Likewise, many wireless sensor networks exist in the network space.

The source sense the data to the destination via one or more wireless sensor nodes as the intermediates. When the source sense the data, it divides the large block of data into finite sized sealed packets. For the purpose of security encryption algorithms can be used by the clients for providing security for its data. As many clients in the form of source outsources their data packets onto the sensor network, the security issues concerning towards data security on network must be paid at most attention. The security is a must as different sources uses different cryptographic techniques to provide security for the data they outsource on to the network.

Security concerns regarding wireless sensor networks have been delt by many authors so far. Dealing with the security at the network level has too major issues to be delt with. The first issue deals with load balancing over the wireless sensor network and the second major issue deals with detection of malicious node on the network. These issues have to be delt by the network administrator.

As described in the above part of the introduction, let us see the composition of a wireless sensor network. A wireless sensor network is composed of finite number of nodes each connected in a wireless fashion. Each sensor nodes consists of head node threat takes a responsibility of load sharing on the wireless sensor network. If the head node is overloaded it forwards the packets to the head nodes of the other wireless sensor network. If all wireless sensor networks are overloaded the packets are queued.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

As mentioned in our paper when the source outsources its field data packets across the network, before doing so the source encrypts the data using deniable encryption which is a strong encryption method where the chances of the hacker getting the original data is very less.

So far we introduced an encryption method which is the primary issue. Coming to the secondary issue load balancing and malicious node detection need to be delt. Load balancing is delt by the head nodes of the wireless sensor networks which forward the data packets to the other wireless sensor networks when its network has been overloaded.

Malicious node detection is our next concern. It is detected taking into considerations two major parameters. They are energy consumption of the network and nodes along with the time consume by each nodes, head nodes in the sensor network to process the data packets they come across.

If the energy consumption and time taken by the nodes in the sensor network is more than the pre-calculated value that is stored, this indicates the presence of a malicious node.

The deniable encryption method and the energy consumption based malicious node detection scheme proposed in our paper is efficient than any other method proposed so far. The major advantage of our paper is the use of deniable encryption.

II. RELATED WORK

In today's various surfing many researching people opinion saying that single network can be implemented by providing authentications and authorizations proving for the network. This may not be a efficient one as this security can be overcome by hacker easily and simply. But in the real world wireless sensor networks are been used to a very large extent that a wireless sensor network performance is degrading day by day. To overcome this single network problem multiple networks are introduced. But the problem still prevails. As an example , at the city of united states of kingdom, many different number of cameras for various networks with different commissions such as police, highway monitoring systems, and locally cities consultants are arrayed on the same old roads [18]. In recent times, some canvassers had been come up with new architecture regarding the cooperation methods for multiple wireless sensors networks in such situations are been brought up. When multiple Wireless sensor networks are constructed in close proximity, they can help each other by forwarding data so that all networks involved benefit from collaborative effort. In [11],the potential benefits of cooperation in multiple Wireless sensor networks are investigated. The authors formulated the system model with objective function and a set of problem constraints. Then,a linear programming framework is used to solve the optimization problem. Since their goal is to investigate the maximum achievable sensor network lifetime with different multi-domain cooperation strategies, optimization objective is network lifetime, which is defined as the time when the first node in a network exhausts its battery and dies.

III. PROPOSED SYSTEM

In this section, we propose a model which balance the load across the Wireless Sensor Networks and ensures data security and data integrity.

Our proposed system model consists of a source, a set of Wireless Sensor Networks and a destination. The source encrypts the data senses the networks around itself forwards the sealed packets across the Wireless Sensor Network in a load balancing manner. In turn each Wireless Sensor Network forwards the sealed packets to its desired destination. In case of presence of malicious node the node is detected as malicious taking into considerations the parameters like lifetime, timeliness and energy dissipation of each node and network is necessary.

``

IV. SYSTEM ARCHITECTURE

In the fig1 we formulate Wireless Sensor Network architecture which is very well load balanced and provides data security and data integrity.

The various components of our architecture are as below

1. Source
2. Destination

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

3. Wireless sensor networks

1. Source:

Source is the element which generates the data to be sent to the destination. Initially before forwarding the data across the networks ,source divides the data of size 'n' into data of size n/2,n/4,n/16 etc. or in any format depending on the size of data. Each block of size 'n' is given a value called hash value which is unique for all the individual data.

Initially the source senses all the various Wireless Sensor Networks available for transmission of its data.As the capacity of each Wireless Sensor Networks are limited using data sheet provided by each Wireless Sensor Networks the source gets the information regarding the Wireless Sensor Networks which are available for its service.

The data to be sent across the networks is divided into blocks of data. AS an example a data block of size,say,20KB is divided into 4 chunks, each of size 5KB and each chunk is given hash value which is same as the hash value of block 'n'.

Before the sealed data packets are outsourced across the Wireless Sensor Networks, it is necessary to provide security for the data. For the same Deniable encryption is furnished, this encryption method encrypts all the chunks of data that are to be forwarded across the network. Now the source forwards the sealed encrypted data across Wireless Sensor Network to which the data is to be forwarded is priory decided by the size thus load is balanced initially.

2. Destination:

This component accepts the data from the source after decrypting the data. As we have accomplished Deniable encryption method there is no chance of destination being not receiving data without data integrity and data security provided at the destination

3. Wireless Sensor Network

This is the component which is responsible for forwarding the source data to the server. Each Wireless Sensor Network consists of fixed number of nodes. The capacity ,timeliness and energy dissipation value of each node is calculated and stored as a prior knowledge. Each Wireless Sensor Network consists of a node called head node. In case, if all the nodes of each network is overloaded the head node in turn communicates with the head nodes of surrounding Wireless Sensor Networks. After gathering head nodes the data sheet values of other Wireless Sensor Networks it forwards the queued or overloaded data to the other Wireless Sensor Networks. The link between the two head nodes is called bridge link. The number of head nodes in each Wireless Sensor Network depends on the number of nodes in that Wireless Sensor Network. Thus this is second situation where the load is balanced over the network. When the sealed data packet encounters each node, depending on the destination address the packets are forwarded to the consecutive nodes. If any node in the network is flooded after accepting data packets the same is intimated to the head node. The head node in turn depending on the destination address forwards the data to the Wireless Sensor Networks via head node. Otherwise the data is sent to the destination itself decrypts the data and extracts original data.

In case of presence of malicious node as it takes more time and dissipates more energy than the actual nodes. This can be notified by comparing the energy dissipated values with the actual node and the malicious node. Obviously time consumed and energy dissipated by the malicious node will be greater than that node is marked as malicious node.

Even though malicious node tries to get the data, if it gets the data, it cannot decrypts and get the original data.In the absence of malicious node the data is securely delivered at the destination. Hence load is balanced across Wireless Sensor Network using head nodes and Deniable encryption enable data security with respect to malicious node.

After going through the architecture and working principles of each module, our paper proposes a system architecture which balances the load across the Wireless Sensor Networks and provides the data security and data integrity via Deniable encryption algorithm.

A. Advantages:

i. Deniable encryption is an hard and inflexible algorithm.
ii. There is no means for the malicious components to decrypt and extract the data.
Load is very well balanced in the both source and Wireless Sensor Network module.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

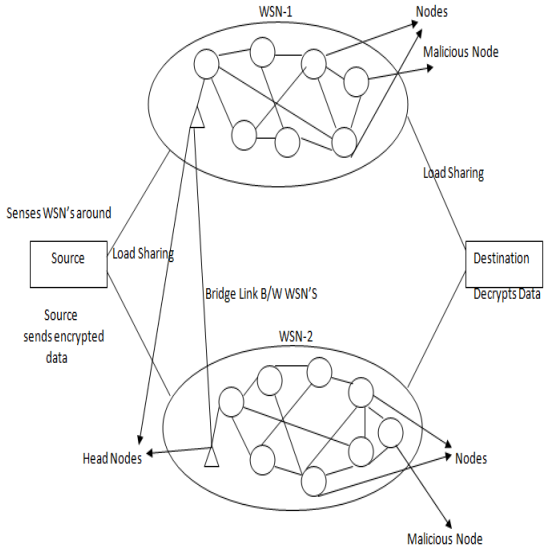


Fig 1 : System Architecture

V. SIMULATION RESULTS

A. Simulation Environment

We evaluated the performance of the proposed method withthe network simulator QualNet 7.1 [24]. We observed thereceiving rate, which is the rate of sensor nodes that send datapackets to their sinks successfully. Therefore, we counted anode that cannot communicate with its sink as a dead node, inspite of its remaining battery. The maximum value of receivingrate is 1.In this simulation model, we set the node configurations
using datasheet and information provided by MEMSIC [25].We simulated four WSNs, WSN 1,WSN2,WSN3 and WSN4 as follows. Each WSN had 49 nodes based on a random topology. The sensing field was a 490 m×490 m square. The PHY model was IEEE802.11b and its data rate was 2 Mbps. The maximum range of radio transmission for each node was 150 m.

Each sink was located at each corner of the field. A shared node was placed at the center of the field. Each node sent 512bytes data packets asynchronously at intervals of 10 seconds. We assumed that sinks and shared nodes had a sufficiently large battery, and that their battery capacities were unlimited. We set x, the cost of using a shared node, to 0.5.To give opportunities for cooperative forwarding to sensor nodes fairly, all nodes deleted their route entries and discovered new routes
at intervals of 720 minutes.

We evaluated two proposed method, *Pool-based* and *Life-based*.For comparison, we simulated an environment wherefour WSNs were operated independently without any cooperation.
In addition, *Energy-based* method was also evaluated as a conventional method. It just focuses on prolonging total lifetime but ignores the fairness among WSNs.

B. Simulation Results

1) Scenario 1: heterogeneous battery capacity: As a basic evaluation for heterogeneity, sensor nodes have differentbattery capacity by a WSN. WSN 1 has the largest capacityand WSN 4 has the lowest. We set the battery capacity of anode in WSN 1 to 1, and the capacity ratio is represented as;WSN1:WSN2:WSN3:WSN4=1:0.75 : 0.625 : 0.5.Note that each node does NOT need to know the initialcapacity of nodes in other WSNs. All each node has to knowis its own initial capacity for operating the proposed method
properly.Figures 6-9 show the receiving rate as a function of elapsedtime for each WSN. They are averaged over 10 trials

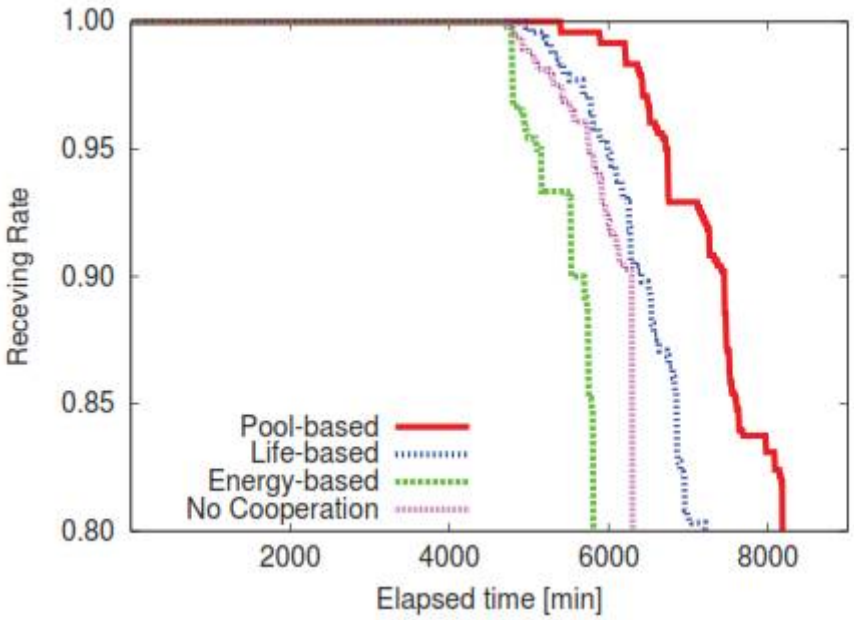
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



V.CONCLUSION

In this paper, we propose a system model that communicates across various Wireless Sensor Networks without overlapping each other and balancing the load passionately. As we have used deniable encryption there is no way provided to the malicious node to decrypt data.

REFFERENCES

[1] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.
[2] M.-S. Hwang, S.-T.Hsu, and C.-C. Lee, "A new public key encryption with conjunctive field keyword search scheme," *Inf. Technol. Control*, vol. 43, no. 3, pp. 277–288, 2014.
[3] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf.*, vol. 4392. Amsterdam, The Netherlands, Feb. 2007, pp. 535–554.
[4] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *J. Netw.Comput.Appl.*, vol. 34, no. 1, pp. 262–267, 2011.
[5] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Inf. Sci.*, vol. 180, no. 13, pp. 2576–2587, 2010.
[6] W.-C. Yau, R. C.-W. Phan, S.-H.Heng, and B.-M. Goi, "Proxy re-encryption with keyword search: New definitions and algorithms," in*Proc. Int. Conf. Security Technol.*, vol. 122. Jeju Island, Korea, Dec. 2010, pp. 149–160.
[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search," *Theoretical Comput. Sci.*, vol. 462, pp. 39–58, Nov. 2012.
[8] W.-C. Yau, R. C.-W. Phan, S.-H.Heng, and B.-M. Goi, "Security models for delegated keyword searching within encrypted contents," *J. Internet Services Appl.*, vol. 3, no. 2, pp. 233–241, 2012.
[9] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," *IEICE Trans. Fundam.Electron.,Commun. Comput.Sci.*, vol. 94, no. 8, pp. 1682–1695, 2011.
[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inf. Sci.*, vol. 258, pp. 355–370, Feb. 2014.
[11] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, "A conditional proxy broadcast re-encryption scheme supporting timed-release,"