Advances in Modelling and Analysis B
Vol. 61, No. 2, June, 2018, pp. 57-63
Journal homepage:http://iieta.org/Journals/AMA/AMA_B

Privacy preservation of sink node location in wireless sensor network using RFSN-RSA

Kolli V. Krishna Kishore*, Pondugala Sudheer Kumar, Dondeti Venketasulu

Department of CSE, VFSTR, Vadlamudi, AP 522213, India

Corresponding Author Email: kishorekvk_1@yahoo.com

Received: April 8 2018
Accepted: June 12 2018

Keywords:
IIOT, wireless sensor network, privacy preservation, adversaries attacks, Random fake sink node, RFSN-RSA, cluster head

ABSTRACT

Sink Node location privacy in sensor networks deployed in Industrial Internet of Things (IIOT) is one of the challenging tasks because of data security and protection. In industrial sensor networks, sensor nodes transfer data packets from a source node to sink node (base station) by using the multi-hop technique. Based on the nature of the sensor network, adversaries may easily track the sink node location by traffic analysis. There are many approaches to overcome this problem. In this paper, we proposed an approach to preserve the privacy of the sink node in addition to secured data transmission from adversaries attacks. In our work, random fake sink node (RFSN) approach is used to mislead the adversary. After forming the clusters, and cluster heads (CH), one of the cluster head will be selected randomly as fake sink node (FSN), and all other CHs send fake data packets to this FSN to mislead adversary. Fake sink nodes are changed dynamically at intervals to make it difficult for an adversary to distinguish between FSN and original sink node. The simulation results show the privacy of the sink node location is preserved from the adversaries with an elongated lifetime of sensor nodes. The simulation result also proved that the proposed approach with RSA algorithm has provided more security with low packet loss.

1. INTRODUCTION

With the evolution of various sensors and latest technologies in the wireless communication, it leads to wireless sensor networks (WSN's) and gaining popularity in Industrial Internet of Things. These are becoming popular in the fields of environmental monitoring, industrial applications, remote surveillance and military war fields. The growth of WSN's is multifold on day by day in the field of signal propagation. In wireless sensor networks (WSN's) sensor nodes are small in size and a large number of nodes are deployed in the network. In a wireless sensor network, each node participates in the transfer of data packets to the neighbor nodes route to the destination, which consumes the energy of a node and increased delay in packet delivery.

In general, most of the applications [10] are using hop by hop communication. The wireless sensor nodes participate in both single hopping and multi-hopping, but single happing consumes more energy than multi-hopping, and multi-hopping communication is also efficiently bypassed signal propagation in wireless sensor network. WSN's are mostly using multi-hopping with the help of routing protocols to forward the packets to the destination using signal propagation. Wireless sensor networks are open nature because each node will freely broadcast the data in the wireless environment that will be vulnerable to eavesdropping. The attackers may use radio transceivers to communicate with WSN's and intercept the message patterns. These message patterns are analyzed by malicious attackers, trace out the path, and identify the location of the sink nodes and source nodes in the network. By using traffic analysis, some of the important characteristics are analyzed in the network. Undoubtedly the crucial aspects of WSN's are energy efficiency, Quality of Service (QoS) (such as End-to-End delay, throughput, and packet loss) and optimal routing.

WSN's in the medical field is used by the physicians to notify the patients for transferring the necessary private data and contextual information for the patient's heart monitoring. By using that information attacker may wrong way to direct the patient's heart problems [1, 3].There are many ways to protect the data from an adversary attacks using preservation of privacy of node location. In the wireless sensor network sink node is the most important node in the network because all nodes collect the data and forwarded to the sink that will maintain all the information about the network. Once the attackers compromise the sink node, they will get the total information about the network. So preserving the privacy of sink node location is one of the finest ways to protect the data from an adversary.

In this work, a new approach is proposed to preserve the privacy of the sink node location. The WSN's clusters are formed with neighborhood nodes, each cluster head transfer of the data to the sink node. In the proposed approach one of the cluster head is randomly chosen as a fake sink node.Using routing policy, all remaining cluster heads transfer the fake data to the selected fake sink node, thereby it misleads the adversaries and protect the original sink node from attacks. The original data from all cluster heads will be anonymously routed to the hidden sink node except fake sink node at that particular time.

2. LITERATURE SURVEY

Yousef Ebrahimi et al., [5] has used multi-hoping to prepare the record of the nodes about an adversary attacks on the network and report to the base station (BS).In the network, BS plays the major role, and it acts as the sink node. An adversary has targeted the sink node location, by using the traffic analysis patterns to detect the sink node location. They introduce transmitting Deceptive Packets in the areas of low belief levels to overcome that problem. So, it flattens the belief curve, thereby making it difficult for an adversary to determine the Sink node, and also keep optimum energy consumption.

Bidi Ying [6] introducing concealing of the sink node location (CSL) by injecting fake packets into the network to prevent attackers in the identification of sink node location through traffic analysis attack. The energy consumption and life time [9] of the wireless sensor networks are strong impacts on the network environment. This paper traces the lifetime, energy-oriented sink node placement in multi-hop and single hop wireless sensor networks respectively. Proposed Ant routing algorithm proved that life time oriented approach outperforms the existing methods in placing sink nodes in Wireless Sensor Networks.

In WSN to detect the sink node location, attackers can use Zeroing-In (ZI) by acquiring the maximum resources from the sink node [7]. Countermeasure of the ZI attack is to forge the ZI attacks, to introduce the Directed Walk based Routing (DWR) method, in which sink node broadcast packets some amount time to mislead attacker. The nature of Wireless sensor networks makes it vulnerable to security, so preservation sink node location is essential as proposed by Devash Pratap Singh et al. [11]. There are many ways to identify the sink node location, such as traffic pattern analysis. The sensor nodes are lesser activity areas spread the fake packets over the network for diverting the attention of the attacker from the analysis of the traffic pattern.

Similarly, in [14] proposed a novel anti-traffic analysis method to preserve the sink‘s location. In this, by focusing either global or local rival, each and every node creates the fake messages. ATA is able to protect the rival from grabbing costly information on the sink's location through the traffic analysis attack. They introduced improved anti-traffic analysis ‘IATA’, which selects few sensors as fake sinks, to protect the sensors all over fake sinks.

Attackers are mainly focusing on the sink node, source node and traffic patterns of the network because of their importance in the network. Abdel et al. [15] proposed a model with fake message injection that can preserve Source location privacy, sink node location privacy and data security against active and passive attacks from local, multi-local and global adversaries.

In YawarBangash et al. [16] proposed MimiBS, which is based mimicking the behavior of Base Station by introducing Aggregator Nods (AN) which will act as Sink Nodes. The performance was evaluated with and without fake packets for privacy preservation of the Base Station. Ring Based Routing (RBR) method addresses the privacy issue of sink node location in [18]. RBR uses the multiple routing rings (MRRs), where nodes are not sending the data directly to the destination sink node, it uses the intermediate rings (neighbor) to transfer the data to the destination node. In this approach, intermediate nodes act as anonymity sink nodes to preserve the privacy of the original sink node. By using the RBR method the routing rings exchange asymmetrical traffic patterns, which mislead the attacker without altering the sink node location.

To achieve high secured location privacy (LP) of both source and sink nodes in WSN’s with low end-to-end latency and low energy consumption in the network H Chen et al. [17] proposed four techniques. These four techniques are ‘Forward Random Walk (FRW)’, ‘Bidirectional Tree (BT)’, ‘Dynamic Bidirectional Tree (DBT)’, and ‘Zigzag Bidirectional Tree (ZBT)’ to deliver the exact data from source to destination and also to achieve the end to end location privacy under local adversary.

Jia-Dong et al. [19] proposed a distributed clustering with a set of non-overlapping K-anonymity aggregate locations for location privacy of sink nodes. They have proposed an algorithm “reciprocal protocol for location privacy (REAL)”, with three key challenges, self-organization, reciprocity property and high accuracy.

SN’s are placed in the different locations. With the help of traffic pattern analysis, sink nodes location are captured. Injecting fake packets in the intersection nodes and forwarding to fake sink nodes was proposed in [20]. The real packet reaches to the destination from the intersection node by the shortest path. This approach countermeasure the adversary in analyzing traffic and misleads in the identification of the real sink node.

Nikolaos Baroutis et al. [21] proposed a Preserve Location Anonymity through Uniform Distribution of Traffic volume (PLAUDIT) approach inject deceptive packets in the network and make difficult for an adversary to find sink node by load balancing the traffic in the network. It is robust in anonymity with low energy consumption and minimum overhead.

Characteristics of the adversary

In cryptography system, an adversary is a malicious object whose aim is to possess the users of the crypto system from accomplishing their needs like integrity, privacy, and availability of data. An adversary's motive is to catch secret data, demeaning small amount of data in the structure, spoofing the uniqueness of a message sender or receiver. In this work, we have simulated adversaries, who attack by analyzing the traffic patterns and find the path to sink node location by gathering information from the sink node.

1. Initially, adversaries are acting like a member network and behaving like a normal node participating in communication and acting as an unbiased decision maker.
2. Adversaries will employ evidence theory to analyze the traffic.
3. An adversary gets initiated with a set of procedural rules.
4. Computationally restricted or unrestrained in terms of storage resources and time.
5. Eavesdropping in the form of passively listening to or actively corrupting data in the channel.
6. Static or adaptive in nature and having fixed or changing behavior.

3. METHODOLOGY

In Wireless Sensor Networks (WSN’s), sensor nodes are randomly deployed. Data sensed in the sensor nodes are forwarded to the Base station (BS), also called as sink nodes, by forming a network with all source nodes, intermediate nodes and sink nodes. Single-hoping and multi-hoping techniques are used to route the packets from source to sink. One of the major drawbacks in WSN is less secure data transmission because of its open channel by nature. By using cryptographic algorithms the data is secured when data is transmitted between the nodes. RSA is the most secure asymmetric algorithm in the cryptography and uses different private and public keys. Initially, every node has a key pair. In case of an attacker tries to intercept the data packets, if key pair values are not matched with the node, then that node will be treated as attacker node. Once, after finding the attacker nodes, they will not be allowed to participate in the transmission of data to the destination (sink node). In the proposed work, a better approach is designed to preserve the privacy of the sink node along with secured transmission from adversaries.

3.1 Network formation

Neighbor nodes (NBNi) are identified in the network from all nodes

Ni = {1,2,3,4,…….N}
Function (NBNi) = get-neighbor-info (Ni) (1)

Initially, all sensor nodes have uniform resources like energy. The energy is consumed in a node while transmitting and receiving the packets. All sensor nodes are grouped into clusters based [8] on the distance between the nodes and energy of each node in the network. In our proposed system highest energy nodes will be considered as cluster heads (CH). CH node will find out the neighbor nodes present in the range (within the threshold) to form a cluster.

get-high-energy (Ni) (2)

where get-high-energy function [21] returns the high energy nodes in the network, that is

CHj = {n7, n20, n24, n27, n10} (3)

By using equation (1), (3) get-neighbor-info function identifies the neighbor nodes by computing distance as given in equation (4). The distance between nodes ‘np’and ‘nq’ are

Dpq= √((x_p-x_q)^2+(y_p-y_q)^2) (4)
p = {1, 2, 3,…..n}, q = {1, 2, 3,…..n}

Based on the equation 5, find out the cluster members CMs

Cj= clusters (CMi) ∀ i = 1 to N (5)
NBNi | Dpq<Rt∀ q, q ϵ Ni

The following is the combination of the different clusters (j=5) with respective cluster members are

Cj={n1,n2,n3,n4,n5,n6,n7} ∪ {n16,n17,n18,n19,n20,n21} ∪{n22, n23, n24, n25} ∪ {n26, n27,n28, n29, n30, n31, n32, n33, n34} ∪ {n8, n9, n10, n11, n12, n13,n14,n15} except n0

Each cluster is formed with the closest nodes with respect to distance. The Highest energy node in the cluster will be selected as cluster head ‘CH’ such as

CH1 = n7, ∀ n7 ∈ C1,
CH2 = n20, ∀ n20 ∈ C2,
CH3 = n24, ∀ n24 ∈ C3,
CH4 = n27, ∀ n27 ∈ C4,
CH5 = n10, ∀ n10 ∈ C5

The data will be transferred to the base station (sink node) with the help of CH’s.

By using LBRA, all possible paths are traced to reach sink node from the CH’s. After that source nodes link to destination nodes, and generated the path. CH’s are ready to transfer the data using the optimum path from all the available paths. All CH’s transfers the fake data to the fake sink node, which is randomly selected from cluster heads to mislead adversary. The original data will be transferred to the sink node anonymously [4], preserves the privacy of sink node.

3.2 Load balancing algorithm

To find the optimum routing path for reducing energy consumption in the sensor nodes, the existing system uses the Carona Load Balancing Routing Tree algorithm (CLBRT). In this algorithm, the optimal path is computed in the network by using the equation (4) to calculate the minimal distance between the nodes, so the energy consumption is at a minimum in the nodes. In this paper, a cluster head is taken as the root node or the parent node in each cluster and the remaining nodes in the cluster are considered as subtrees or next level of nodes ‘L’. Find-Min function is used to find the minimum distance with low traffic routes in the subtrees. After finding out the path the data packets will be transferred from cluster members to the cluster head. The base station follows the greedy method to form the LBRA and alert to the parents in the topology using improved load balancing routing tree algorithm (Improved-LBRA). The basic goal of improved-LBRA is to transmit data packets to sink node in a more healthy way. Moreover, nodes produce fake data packets at the estimated data rate and transfer to the fake sink node.

3.3 Data security with RSA algorithm

The RSA algorithm is mostly used an asymmetric key cryptographic algorithm with variable key sizes. In the proposed approach, the RSA algorithm with a key size of 1024 is used to make it difficult for an adversary to break the key, as mostly they have limited computing facility available to them on the field. In this RSA algorithm, two different keys are used, one is public key another one is a private key. In our proposed work, these two keys are related to each other and randomly generated with the help of Random key generation function. In this work, each node having a pair of keys that will be maintained by the two directories, public key directory, and the private key directory. The relation of the key pairs should be preserved by the directories. These two directories are working under the base station.

Working of RSA algorithm:

1. Considering the two prime numbers ‘p’ and ‘q’, and p is not equal to q ($p \neq q$).
2. Computing the ‘n’ value from the p and q

n = p * q (6)

3. Calculate the ϕ value with the help of p and q values

ϕ= (p-1) * (q-1) (7)

4. Find out the exponent of the public key (PUK) ‘e’ value between 1 and ϕ

i.e., $1 < e < \phi$,

Moreover 'e' and ϕ are co-primes and find out the

$$\mathrm{gcd}(e, \phi) = 1. \tag{8}$$

5. Find out the exponent of the private key (PRK) 'd' with the help of the following equation

$$(d * e) = 1 * \mathrm{mod}\ (\phi) \tag{9}$$

6. Public key and private keys from above equations are (n, e), (n, d).

7. Encryption performed on packets transferred from source nodes

$$c = \mathrm{pow}\ (m, e) * \mathrm{mod}\ (n) \tag{10}$$

where 'c' is Cipher text

8. Decryption of packets are performed in Sink node

$$m = \mathrm{pow}\ (c, d) * \mathrm{mod}\ (n) \tag{11}$$

where 'm' is the original message.

In our proposed system RSA algorithm is used to generate key pairs. By using these two keys PUKi (i=1,2,3,…….,n) and PRKj (j=1,2,3,…….n) each node in the network is to be verified/identified

$$Ni \in \mathrm{verify}\ (\mathrm{Rand}\ (PUKi), \mathrm{Rand}\ (PRKj))\ PUKi\ R\ \ PRKj \forall\ i=j \tag{12}$$

where 'verify' function used to verify the key pairs and 'R' is the relation between PRK and PUK.

3.4 Energy consumption model

Energy consumption in the modeling phase [9, 13] is computed for information transmission and reception based on the radio propagation signals. Let ET and ER represents the energy consumption of both transmitting and receiving s-bit data over the D distance.

Sender side (transmission)

$$ET\ (s, D) = ET\text{-}elec * s + ET\text{-}amp * (s, D), \tag{13}$$

$$ET\ (s, D) = Eelec * s + \varepsilon amp * s * D2, \quad D < D0. \tag{14}$$

Receiver side (receiving)

$$ER\ (s) = ER\text{-}elec * s, \tag{15}$$

$$ER\ (s) = Eelec * s \tag{16}$$

where D is the transmitting distance,
ET-elec is the energy consumed by the transmitter,
ER-elec is the energy consumption of the receiver and
ET-amp is the amplification coefficient.

3.5 Misleading the Adversaries

Let N be the number of sensor nodes, and i represent the node (i = 1, 2, 3,….., N) is arranged autonomously at (Xp, Yq) in the zone Z. With the help of these nodes to form clusters Cj(j = 1, 2, 3, 4, 5), and each cluster having the maximum number of sensor nodes are dependents on CH for transmitting the data to the destination. In each cluster having one cluster head node CHj, every operation in the cluster will take care by the cluster heads and reaming nodes are in an ideal state.

In the proposed system after forming the clusters, CHs are used to transfer the data to the base station or sink node.

$$Z\ (Xi, Yi) = CHj \in Cj\ (D) \rightarrow SN \tag{17}$$

where 'D' represents the data and
'SN' represent the sink node of the network.

The CHs are collecting the data from the cluster members.

$$CMs\ (D) \rightarrow CHj(D) \tag{18}$$

where, CMs represent the cluster member.

One of the cluster head is randomly selected and will act as the fake sink node. So remaining cluster heads transfer the fake data to the fake sink node to mislead adversaries.

$$\mathrm{Rand}\ (CHj) \cong FSN \rightarrow [FSN \nexists CHj](FD) \tag{19}$$

where FSN represents the fake sink node, FD represents the fake data and Rand represents the random function to select one of the CH nodes in Z.

Except for the fake sink node, remaining cluster heads transfer the original data to the sink node anonymously.

$$[\mathrm{Rand}\ (CHj) \neq FSN](D) \rightarrow SN \tag{20}$$

Fake sink node (one of the cluster head) also transfers the original data to the hidden sink node.

$$FSN\ (D) \rightarrow SN \tag{21}$$

The fake sink node and original data transferring node should be selected randomly.

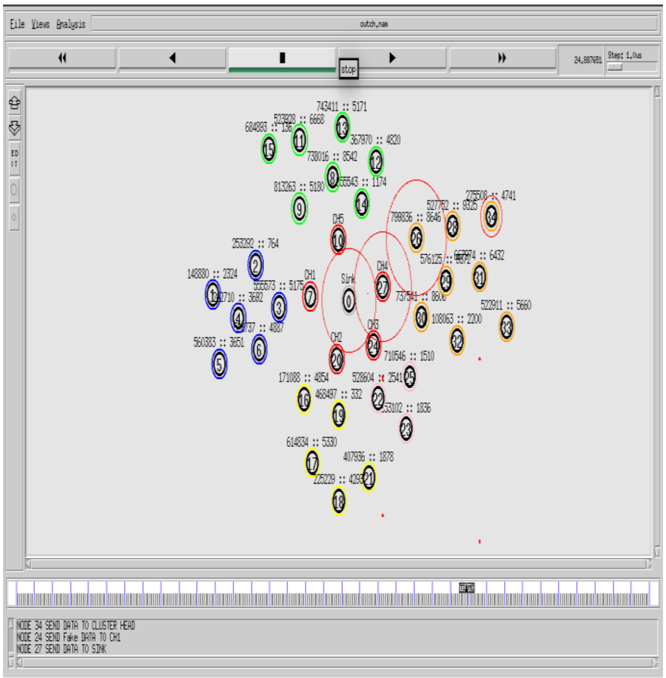
$$\mathrm{Rand}\ (FSN \in CHj), \mathrm{Rand}(FSN \nexists CHj) \tag{22}$$

In this system the sink node should be hidden by using GPS location hiding techniques, to provide the location privacy of the sink node for secured data transmission.

The proposed method ensures privacy preservation of sink nodes from the adversary attacks and secures transfer of data from source nodes to sink node or destination node using RSA algorithm.

4. SIMULATION RESULTS

In the simulation we have used the NS2 simulator tool to validate the performance [2] of the RFSN-RSA. In the simulator, a wireless sensor network with the area of 1000x1000 meters is simulated. In this WSN, 35 sensor nodes are deployed randomly over the network and the simulation time is set to 35.00 seconds. Sink node (base station) is placed in the middle of the network, at a position 0 (1024, 664). In this network the packet size of each node is 1000 and the data transmission rate of the network is 512 kb.



NODE 34 SEND DATA TO CLUSTER HEAD
NODE 24 SEND Fake DATA TO CH1
NODE 27 SEND DATA TO SINK

Figure 1. Transformation of original data to a sink node

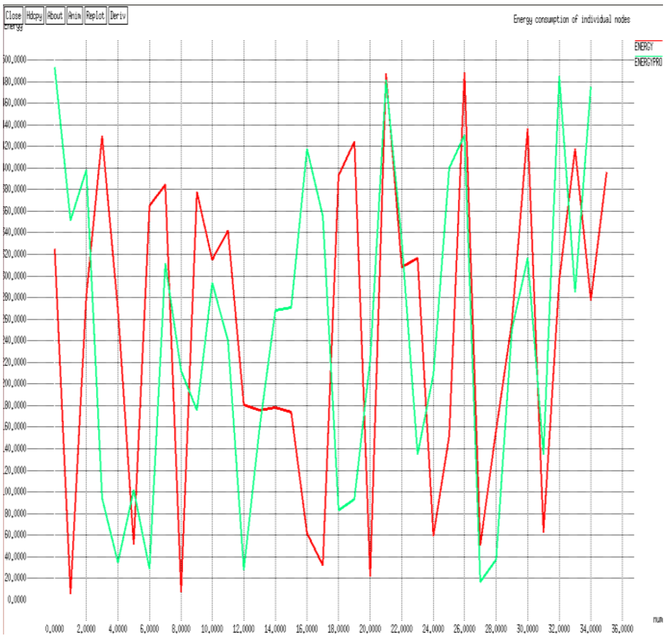


Figure 2. Energy consumption of each node

Initially, all sensor nodes are having a certain amount of energy. After the end of the simulation, each node will lose some amount of energy because of energy consumption for packet delivery. In the proposed system, cluster heads are selected based on the amount of energy in the cluster. Then sink node location is made hidden for preserving the privacy of the location of the sink node to mislead the adversaries. The metrics used for performance evaluation in this simulation are packet loss, end-to-end delay, packet delivery ration, consumption of energy for the whole network and individual nodes in the network. These metrics are used to compare the proposed approach RFSN-RSA with the existing system 'PLAUDIT'. The proposed system outperformed the existing system as given in the following section.

The above graph shows energy at each node and the comparison between the existing system (PLAUDIT) and the proposed system. The x-axis represents the total simulation time for the data transmission from source to sink node in seconds and the y-axis shows the consumption of the energy at each node in terms of joules.The proposed system results are better when compared to the existing system(PLAUDIT) because in the proposed system mostly cluster heads are participated in the data transmission while remaining nodes are in the idle state.

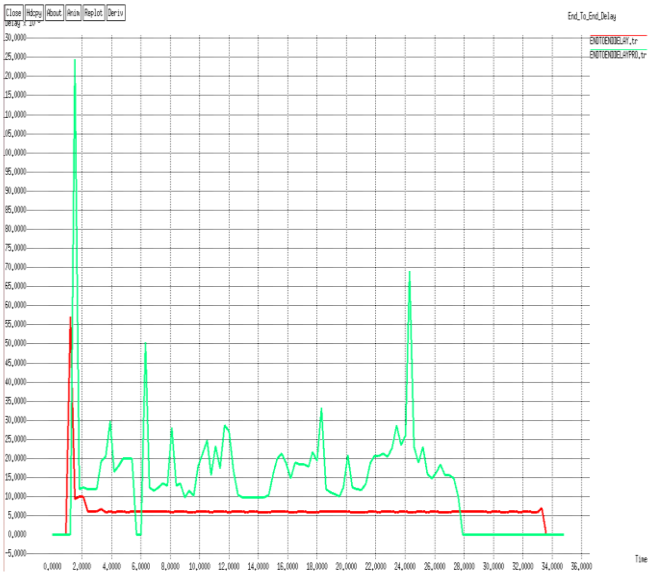


Figure 3. End-to-End delay

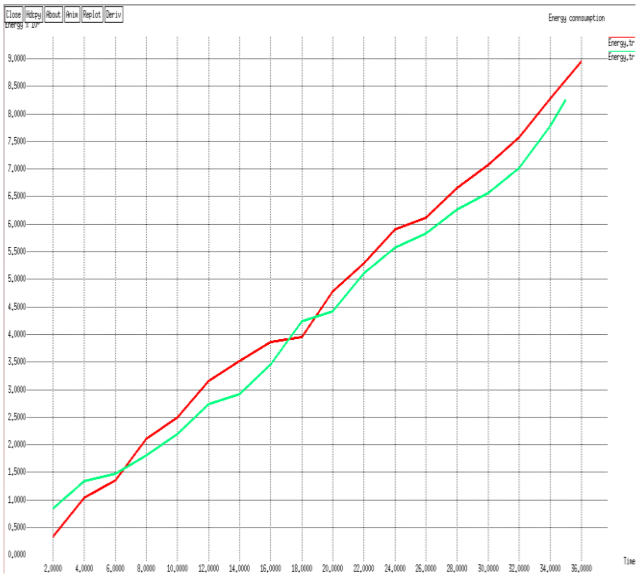


Figure 4. Energy consumption of the whole network

The above graph represents an end-to-end delay between the existing system and the proposed system. During the data transmission time gap will be occurred between the nodes. The time delay in the proposed system is more when compared with the existing system, because of the proposed system mislead the adversaries by the participation of more numbers of intermediate nodes in data transmission. In this graph, the x-axis represents the total simulation time in seconds and the y-axis represents the delay time in seconds.

The Figure 4 represents the total energy consumption of the whole network. In the proposed system consumption of energy is less compared with the existing system. In our proposed system cluster heads will perform most of the operations during the data transmission. In the above graph, the x-axis represents the total simulation time in seconds and they-axis represents the energy consumption in joules.

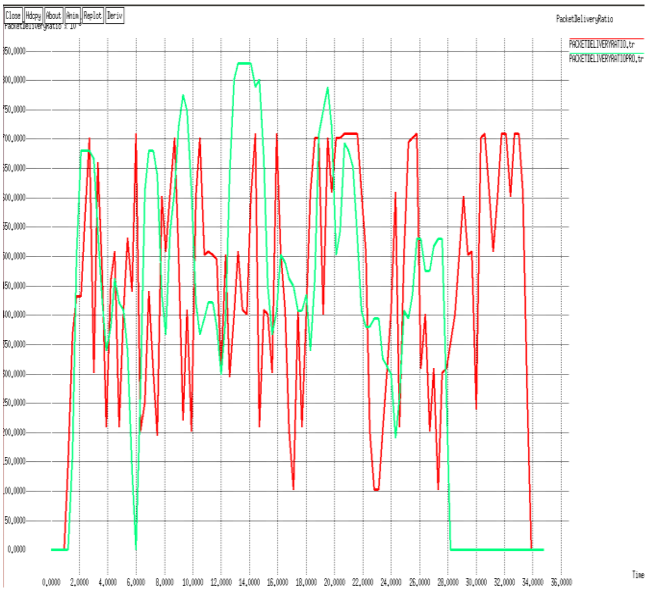


Figure 5. Packet delivery ratio

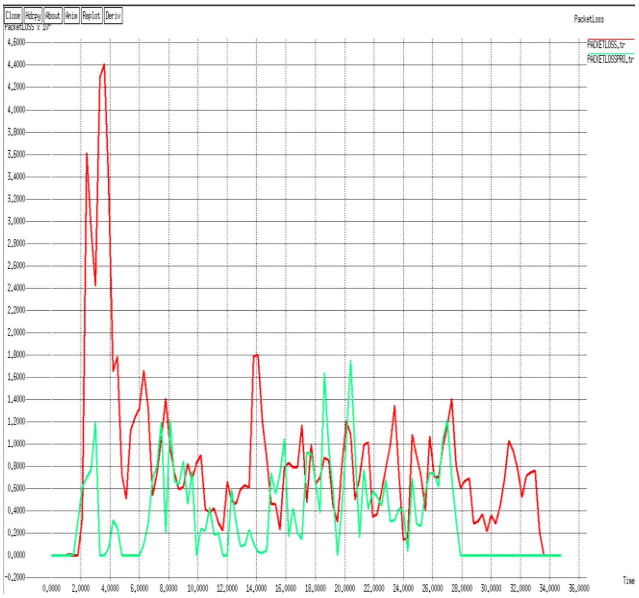


Figure 6. Packet loss between source node destination node

Figure 5 represents the packet delivery ratio (PDR) for the whole system during the data transmission. The PDR of the proposed system more appropriate compared with the existing system. In the proposed system, even with more complexity, still throughput is high when compared to the existing system. In the above graph, the x-axis represents the total simulation time in seconds and the y-axis represents the packet delivery ratio. Packet delivery is the number of packets/bytes received per unit time.

The graph shown in Figure 6. represents the packet loss, the dropping of the packets during the data transmission. Packet loss of the proposed system is less compared to the existing system, because use of RSA algorithm prevents packet capture by adversaries. In the above graph, the x-axis represents the total simulation time in seconds and they-axis represents the number of packets dropped per unit time.

5. CONCLUSION

In this paper, we have mainly focused on minimization of packet drop, analyze the traffic,reduce usage of energy and mislead the adversaries. Our approach defended the attacks in two phases. The first phase verifies the attackers by using RSA algorithm for each node in the network. The second phase is to mislead the adversaries with a randomized selection of fake sink node, by including fake data packets from different cluster heads. The main goal of RFSN-RSA is for privacy preservation of sink node against adversary attacks. Simulation results show that the proposed approach provided better privacy of the sink node location from the adversaries than existing methods with an improved lifetime, low packet loss, and high delivery of the packets. The simulation result also proved that the proposed approach with RSA algorithm has provided more security than existing system.

REFERENCES

[1] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. (2002). Wireless sensor networks: A survey. Computer Networks 38(4): 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

[2] Hansen E, Neander J, Nolin M, Bj M. (2009). Efficient Cluster Formation for Sensor Networks, 1–8.

[3] Li N, Zhang N, Das SK, Thuraisingham B. (2009). Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks 7(8): 1501–1514. https://doi.org/10.1016/j.adhoc.2009.04.009

[4] Poe WY, Schmitt JB. (2009). Sink placement without location information in large-scale wireless sensor networks. Asian Internet Engineering Conference 69-76. https://doi.org/10.1145/1711113.1711126

[5] Ebrahimi Y, Younis M. (2011). Using deceptive packets to increase base-station anonymity in wireless sensor network. In 2011 7th International Wireless Communications and Mobile Computing Conference, IEEE 842–847. https://doi.org/10.1109/IWCMC.2011.5982656

[6] Ying B, Gallardo JR, Makrakis D, Mouftah HT. (2011). Concealing of the sink location in wsns by artificially homogenizing traffic intensity. In 2011 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2011. https://doi.org/10.1109/INFCOMW.2011.5928957

[7] Liu Z, Xu W. (2012). Determining sink location through Zeroing-In attackers in wireless sensor networks. Wireless Networks 18(3): 335–349. https://doi.org/10.1007/s11276-011-0403-2

[8] Wang G, Kim D, Cho G. (2012). A secure cluster formation scheme in wireless sensor networks. International Journal of Distributed Sensor Networks 2012. https://doi.org/10.1155/2012/301750

[9] Chen F, Li R. (2013). Sink node placement strategies for wireless sensor networks. Wireless Personal Communications. https://doi.org/10.1007/s11277-011-0453-x

[10] Ngai ECH, Rodhe I. (2013). On providing location privacy for mobile sinks in wireless sensor networks. Wireless Networks 19(1): 115–130. https://doi.org/10.1007/s11276-012-0454-z

[11] Singh DP, Goudar RH, Wazid M. (2013). Hiding the sink location from the passive attack in WSN. In Procedia Engineering. https://doi.org/10.1016/j.proeng.2013.09.072

[12] Al-Haija QA, Smadi M, Al-JA'Fari M, Al-ShuA'Ibi A. (2014). Efficient FPGA implementation of RSA coprocessor using scalable modules. Procedia Computer Science 34(Eicm): 647–654. https://doi.org/10.1016/j.procs.2014.07.092

[13] Jain TK, Saini DS, Bhooshan SV. (2014). Cluster head selection in a homogeneous wireless sensor network ensuring full connectivity with minimum isolated nodes. Journal of Sensors 2014. https://doi.org/10.1155/2014/724219

[14] Ying BD, Makrakis D, Mouftah HT. (2014). Anti-traffic analysis attack for location privacy in WSNs. https://doi.org/10.1186/1687-1499-2014-131

[15] Abuzneid AS, Sobh T, Faezipour M. (2015). An enhanced communication protocol for location privacy in WSN. International Journal of Distributed Sensor Networks 2015. https://doi.org/10.1155/2015/697098

[16] Bangash Y, Zeng L, Feng D. (2015). MimiBS: Mimicking Base-Station to provide location privacy protection in wireless sensor networks. Proceedings of the 2015 IEEE International Conference on Networking, Architecture and Storage, NAS 2015 158–166. https://doi.org/10.1109/NAS.2015.7255210

[17] Chen H, Lou W. (2015). On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. Pervasive and Mobile Computing 16(PA) 36–50. https://doi.org/10.1016/j.pmcj.2014.01.006

[18] Long J, Liu A, Dong M, Li Z. (2015). An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing. Journal of Parallel and Distributed Computing 81–82, 47–65. https://doi.org/10.1016/j.jpdc.2015.04.003

[19] Zhang JD, Chow CY. (2015). REAL: A Reciprocal Protocol for Location Privacy in Wireless Sensor Networks. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2014.2366467

[20] Wang J, Wang F, Cao Z, Lin F, Wu J. (2017). Sink location privacy protection under direction attack in wireless sensor networks. Wireless Networks. https://doi.org/10.1007/s11276-015-1179-6

[21] Baroutis N, Younis M. (2017). Load-conscious maximization of base-station location privacy in wireless sensor networks. Computer Networks 124, 126–139. https://doi.org/10.1016/j.comnet.2017.06.021

[22] Sirajuddin M, Rupa Ch, Prasad A. (2018). A trusted model using improved-AODV in MANETS with packet loss reduction mechanism. Journal of Advances in Modelling and Analysis B 61(1): 15-22.

[23] Liyanage M, Chang C, Srirama S, Loke S. (2018). Indoor people density sensing using Wi-Fi and channel state informatin. Journal of Advances in Modelling and Analysis B 61(1): 37-47.