Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 32 (2014) 1174 – 1179

Procedia Computer Science

International Workshop on Wireless Networks and Energy Saving Techniques (WNTEST-2014)

Novel Scheme of Fuzzy Based Concealing Sink Node with Fake Holes (F-CSH)

Ahmed E. El-Din[a], Rabie A. Ramadan[a], A. A.Elmagid[b] and Salah A. Aly[c]

[a]*Computer Engineering Department, Faculty of Engineering, Cairo University, Cairo, Egypt.*
[b]*Electronics lab-physics department, girls collage for Art, Science and Education-Ain Shams University,Cairo, Egypt.*
[c]*Smart Networks Lab, College of Computer and Information Systems, Umm Al-Qura University, Makkah, KSA*

Abstract

Due to the sink node crucial position, its location privacy is becoming one of the major issues in wireless sensor networks (WSNs) which requires ultimate protection. Particularly, the WSNs successfulness is endanger as the wireless transmission nodes are susceptive to illicit tracing and detection. While privacy of the message can be ensured through encryption content, this paper formalizes a novel efficient privacy preserving scheme to secure sink node location. The aim is to keep the location privacy of the sink node from being tracked using the traffic flow passive analysis. F-CSH is based on the concealing of the location of the main sink using fake sink holes been elected using fuzzy score function. In addition, comprehensive simulations proved that the proposed scheme significantly upgrades both delivery time and conservation energy cost compared with existing strategies.

Keywords: **Location Privacy, Fuzzy Logic, Concealing in WSNs.**

1. Introduction

Recently, with the remarkable advance of electronic systems fabrication, there has been increased interest in Wireless Sensor Networks (WSNs) [1], [2]. Due to the bright and interesting future promised the world of information technology, WSNs have been technically identified as one of the most important technologies to be envisioned in different critical applications including military and civilian monitoring [1], [3], [4].

A WSN typically consists of large number of distributed small, cheap, constrained energy and computational utilities sensor nodes. Sensor nodes cooperatively pass their data through the sensor network to the

[a] Corresponding author. Tel.: +201067643227.
E-mail address: rabie@rabieramadan.org

doi:10.1016/j.procs.2014.05.550

most powerful node named main sink node or Base Station (BS) to be processed [5]. In spite of WSN popularity, any failure or physical attack exposure to BS leads to collapse of the entire sensor network [6]. Due to the open nature of WSNs, wireless communications are relatively vulnerable to be intercepted in an unauthorized manner, eavesdropped and traced by adversary [7].

More specifically, privacy threats in sensor networks are classified into two categories: data packets privacy, and contextual privacy [8]. In the case of data packets privacy, threat adversary can detect and tamper the packets sent over the network. Although message confidentiality can be countered through intensive cryptographic of the packets content instead of real identities, it is possible for the adversaries to identify and monitor the intensity of the communication patterns with an appropriate radio receiver no matter whether messages are encrypted or not. Concerning contextual privacy, it deals with the protection of the context associated with broadcasting of sensitive data such as the location of the message originator, the generated message time, locations of monitored objects and BS etc. Moreover, in the worst case, an anonymous may be able to undetectably take control of some sensor nodes, inject false data packets or reprogram the sensor nodes [9], [10].

Additionally, because of scarce energy in WSNs domain, concealing the location privacy became an extremely challenging task. Otherwise, the WSNs can be exposed to malicious traffic analysis and accordingly the significant contextual information to be carried out and exploited by an adversary. Therefore, sink nodes location privacy requires ultimate protection. Generally two methods for unauthorized sink locating with no access to the message content but message existence: *traffic-analysis* and *packet-tracing*. It is based on that the sensors closer to the BS receive and transmit greater volume of packets than sensors further away from BS. Obviously, the location of the sink is inferred based on the traffic densities analysis of different locations. This process takes long time as the adversary has to move from location to location and stay at each location long enough such that sufficient data can be gathered for computing the traffic rate [11]. Considering packet-tracing, transmission link could be revealed when tracing the transmitted consecutive packets by nodes towards sink. When a traditional single-path routing protocol is implemented, the network is extremely vulnerable to the packet-tracing attack, since the routing paths are specified and directed to the sink. By eavesdropping, an adversary is able to perform hop-by-hop tracing along path towards the receiver for each packet overheard.

In this paper, we focus on studying concealing the sink node location with the efficient scheme in-terms of the safeguarding sink location privacy against threats with acceptable energy consumption. We proposed a novel scheme named fuzzy based concealing for sink node using fake holes (F-CSH). The proposed scheme is based on creating dummy sink holes to be elected by nodes to mislead attackers and enhance the sink privacy strength with random selection of neighbour for the real packet transmission each time. Under such a protection scheme, an adversary can't identify the right direction to reach the real sink [12]. Moreover, simulation results also are carried out to demonstrate the efficient of the proposed scheme in protecting the location of the sink with efficient power consumption. The remainder of the paper is organized as follows: Section 2 summarizes related privacy works in WSNs. Section 3 explains the statement of system models followed by the description of the scheme of protecting the sink location privacy in section 4. Section 5 evaluates the simulation results and performance analysis and the overhead of the privacy protocol. Finally, section 6 concludes the paper.

2. Related work

In WSNs, there are different representative schemes for source-location node's privacy. Bidi Ying et. al. in [13] proposed a Concealing of the Sink Location (CSL) technique, which is based on the use of fake message injection. CSL starts with topology discovery phase where the sink broadcasts encrypted message and the intermediate nodes forward only one copy of such an encrypted message. Several nodes are randomly selected to generate Fake messages of the same size to disable monitoring the traffic volume. After a tree-like structure has been generated and during the data transmission phase, CSL instructs each node to send the same number of messages. Therefore, the attacker cannot identify the sink node. Obviously this scheme consumes the limited node's residual energy and decreases the overall network's lifetime.

Deng et al. [14] proposed Differential Enforced Fractal Propagation (DEFP) against traffic analysis attack for BS location privacy, where every node in the network has to transmit messages at a constant rate. However, the traffic-analysis attack is not a preferable measure for an adversary. In addition, this approach introduced extra delay for delivering packets. Xinfeng Li et al. [15] centralized scheme is based on several fake packets injection to conceal the real packet during data transmission period. BS randomly selects a common node to be the pseudo BS. However,

randomization leads to much longer packet delivery latency and heavier workload in addition to more energy consumed if the nodes are away from the pseudo BSs. Our proposal in this paper tries to solve the problems of the previous schemes through fake sink node.

3. Statement of system models

In this section, the sensor network and adversary models are defined; then a new scheme for protecting sink node location privacy is proposed.

Sensor network model: The monitored space A is described as a 2-D environment, with length L and width W. The WSN densely randomly deployed is composed of one sink and large number of homogeneous and immobile sensors with limited energy and computation capabilities. Without loss of generality, one sink is assumed in the network to collect data packet where it can be easily extending to multiple sinks. These sensors can communicate with each other directly or indirectly based on the distance and transmission range. In addition, sink node is assumed to have sufficient computation and storage capabilities to collect the sensed data packets via various neighbouring nodes. Furthermore, the proposed system has the following assumptions: The content of data packet will be guaranteed by an encryption technique for keeping the message secure. However, the encryption process is beyond paper scope [16], [17]. The node concatenates several data packets received from different nodes and then resubmit the result as a new packet. Hence, every packet delivered in the network has the same packet size thus the hacker cannot pinpoint the sink location for the size of the data packet. The sink node is assumed to passively receive packets with no rely on sending requests.

Adversary model: The adversary's model is assumed to be able to perform traffic-analysis and packet-tracing attacks, with the following features: The adversaries have appropriate computation capability and sufficient data storage memory; while being equipped with supporting devices. The attacker can't get the content of the packets caused by encryption; thus unable to distinguish between original and fake messages. The attacker doesn't actively interfere with regular network communications but can passively monitor and eavesdrop the communication channels to remain untraced and hidden from the network operator.

4. Novel Scheme of Fuzzy Based Concealing Sink Node with Fake Holes (F-CSH)

Fuzzy logic concept is almost derived from the theory of fuzzy sets which related to objects classes with un-sharp boundaries where membership or truth of any statement is a matter of degree. Fuzzy logic was first introduced by Lotfi A. Zadeh in the mid-1960s for representing uncertain and imprecise knowledge [18]. It provides an approximate but efficient means of describing the behaviour of systems that are too complicated, ill- specified, or not easily analyzed mathematically. As considered before, N heterogeneous are randomly deployed nodes. All sensors generate m messages with the same size L bits. In this section, we introduce our concealing scheme (F-CSH). F-CSH is based on using fake sink holes -elected using fuzzy score function- to keep the location privacy of the sink node from being tracked using the traffic flow passive analysis. F-CSH also introduces additional difficulty on the traffic analyzers by selecting random neighbours for forwarding the real packets. Our proposed algorithm starts with Neighbours discovery. Then, the network lifetime is divided into rounds; each round is composed of two phases, ***fake sink holes announcement phase*** and ***Data delivery paths phase*** as follow:

Phase 1 "Neighbours discovery": Directly after deployment, the sink node broadcasts identification message holding the *id,* as shown in equation 1. Each node, using the RSSI (Received Signal Strength Indication) of this message [19], estimates how far from the sink node. This can be easily extended to multiple sink networks. Then, as shown in equation 2, each node broadcasts message holding the node's own identifier (*id*) and the distance to the sink node (*d*), with limited power to be heard by the neighbour nodes (*M*). Neighbour nodes save the received information to be used in further routing. Equation 2 is for node i, with identifier id_i, distance from sink d_i and neighbour nodes M_i.

Phase 2 "Fake Sink holes announcement": During this phase, nodes calculate their fuzzy score. The fuzzy variables considered in our proposal are: the *residual energy* which is the current energy of the node, *connectivity factor* be the number of neighbour nodes and the *centrality factor* as the average summation of the distances between the node and neighbour node. Equation 3 shows the centrality factor of node i, where M_i is the number of

neighbour nodes for node *i* and d_{ij} be the distance between node *i* and neighbour node *j*.

$$Sink\ (id_{sink}) \rightarrow Nodes \quad (1) \qquad Node_i\ (id_i \mid d_i) \rightarrow M_i \quad (2) \qquad CF_i = (\Sigma_{1<j<Mi}\ d_{ij}) / M_i \quad (3)$$

Nodes broadcast their fuzzy score, with the highest be the fake sink holes of the current round. Other nodes select their fake sink holes based on the fuzzy score or RSSI [19]. The used linguistic variables for the crisp input are limited to three variables which are *low, medium and high* for the residual energy and connectivity factor while *far, adequate and close* confined to centrality factor as shown in Fig. (1). The fuzzy set for the output which is the score of the node is represented using five linguistic variables which are *very low, low, medium, high, and very high*. Defuzzification process is done by Center of Gravity (COG).

Phase 3 "Data delivery paths": F-CSH assumes multi-hop network with no direct path from node to the real sink node. Nodes send multi-casted packet holding the address of its fake sink hole and randomly one of the nearest neighbours to the targeted real sink node. This process is declared using the multi-casted destination equation 4, where FSi is the fake sink selected by Nodei for the current round and RMi is the randomly selected neighbour for Nodei. Thus the size of the data packet sent to the fake sink hole is of the same size that sent to the random neighbour, thus the traffic analyzer cannot identify the real sink form the packet size. This method is repeated by the intermediate nodes on the path from the source node to the real sink. This introduces different paths in each time, in addition to different fake sink holes by each new *fake sink holes announcement* phase. The intelligent fake node selection approaches is presented in Fig. (2), as shown, *s* be the source sensor node, randomly selected one of its near neighbour nodes to the real sink. The figure shows the repeating of the data delivery, where each neighbour node also randomly select one of its near neighbour nodes to the real sink then forward the data to the selected neighbour and the selected fake sink hole. Figure (3) summarizes the 3 phases of the proposed F-CSH scheme.

$$Node_i\ (Data) \rightarrow (FSi, RMi) \quad (4)$$

5. Simulation Results and Performance Analysis

In this section, we evaluate the performance of the proposed scheme. Experiments are performed on our own simulation written on *Matlab*. In our simulation, we use *N* as the number of nodes N=1000 deployed in an area A=1000 x 1000 m^2. Nodes transmission range is set to *L=150m*. The initial energy of the node is assumed to be *10J*. In addition, for simplicity, the size of the message sent by a node as well as the aggregated message from the intermediate nodes is set to 4000 bit message. To test our proposal in this paper, the selected energy model follows the footsteps the one proposed in [20]. The energy expended for $Node_i$ during transmission of a *M* bit message for a distance *d* is as shown in equation (5), On the other hand, energy expended during receiving *M* bit message is as shown in equation (6).

$$E_{TX}(M,d) = E_{elec} \cdot M + E_{amp} \cdot M \cdot d^{Y} \quad (5) \qquad E_{RX}(M) = E_{elec} \cdot M \quad (6)$$

where E_{elec} is the energy dissipated by turning the radio circuit for either sending or receiving and its value is equal to 50 nJ/bit. E_{amp} is the energy dissipated using the transmitter amplifier and its value is equal to 100 pJ/bit/m^2. *Y* is the path loss exponent and equal to 2. Let for $Node_i$, K_i be the sub-set of neighbour nodes M_i that are the nearest to the sink node and V_i be the nearest sub-set of the available FSH_r (fake sink holes) for the current round (*r*), as shown in equation (7). *K* is application dependant variable, bigger *K* value results in higher concealing probability.

$$K_i \subseteq M_i \text{ and } V_i \subset FSH_r \quad (7)$$

For the current round, the number of unique combinations for $Node_i$ to select for mulit-casted packet is ($K_i.V_i$). While the probability for $Node_i$ to select certain fake sink hole is ($1/|V_i|$) while the probability to select certain neighbour node for forwarding the current data to the real sink is ($1/|K_i|$). Thus the probability to select certain pair (fake node, neighbour node) is ($1/(V_i \cdot K_i)$). With probability of certain set of pairs be selected starting from the source node to the sink be as ($1/(\prod_{SourceNode<j<Pre\_sink} (Vj \cdot Kj))$). Let d_i be the distance from the source node ($Node_i$) to the sink, in terms of hop count. Thus (d_i-1) neighbour nodes along this path will follow the data path delivery phase by selecting fake sink hole and real neighbour to the real sink. With ($2.d_i$) packets been generated, d_i packets for the fake sink holes and d_i packets for the real path. The number of the unique paths, form the source node ($Node_i$) to the sink be (d_i+1), one real path with (d_i) fake paths, with probability to follow the real path be ($1/(d_i+1)$). This probability mainly depends on the path length and the number of nodes in both sets; and decreases dramatically for the random selection of the next neighbour in each *Data delivery paths* phase and the random change of the fake sink holes each *Fake Sink holes announcement* phase.

Consider CSL scheme described above, several nodes are randomly selected to generate fake messages of the

same size to disable monitoring the traffic volume. After a tree-like structure has been generated and during the data transmission phase, CSL instructs each node to send the same number of messages. Therefore, the attacker cannot identify the sink node. CSL is selected as the authors followed the same idea of generating fake packets. Obviously, this scheme consumes the limited node's residual energy. Based on the previous setup, Figures 3 shows the average residual energy (the average of the residual energy of all nodes in the network) per iteration using the proposed scheme F-CSH and CSL with different configurations of the number of messages sent by every node. As shown in the figure, the proposed fuzzy scheme decreases of the average residual energy in acceptable way compared to the stated CSL that forces each node to send the same number of messages like the nearby nodes to the sink node.

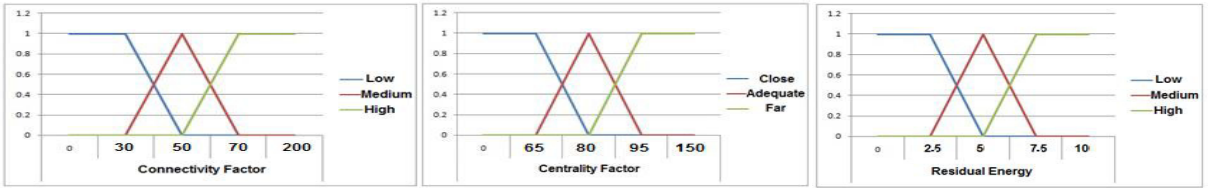

Fig. (1): Membership Functions for input parameters.

Input: A sensor network with $S = \{s_1 \ldots s_n\}$ source nodes, n source packets x_{si} ,....., x_{sn}.
The sink node broadcasts identification message
Phase 1 "Neighbours discovery": **foreach** $node_i$ do
1. Estimate how far from the sink node using the RSSI.
2. Broadcast to the neighbor nodes, the identifier and the distance to the sink node.
3. Neighbor nodes save the received information to be used in further routing.

Phase 2 "Fake Sink holes announcement": foreach *nodei* do
1. Calculate then broadcast the fuzzy score.
2. The highest fuzzy score nodes be the fake sink holes of the current round.
3. Other nodes select their fake sink holes based on the fuzzy score or RSSI.

Phase 3 "Data delivery paths": foreach *For all intermediate nodes on the path to the real sink* **do**
Send multi-casted packet for the selected fake sink and the randomly nearest neighbors.

Algorithm 1: Fake Sink Node algorithm

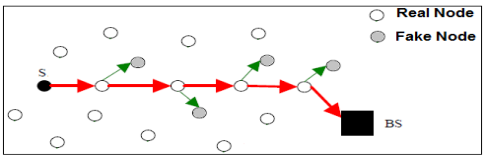

Fig. (2): Intelligent fake node selection approaches.

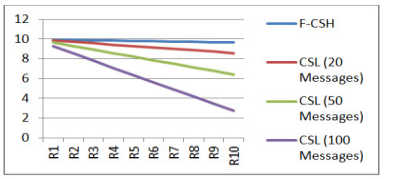

Figure (3): The Average energy of the node comparison.

6. Conclusions

In this paper, we proposed a novel privacy-preserving scheme applying intelligent fake sink node topology to protect the location privacy of BS. In which, F-CSL based on the concealing of the main sink using fake sink nodes been elected using fuzzy score function. Based on, the sink location could be parasitized with dummy sink nodes. The carried out simulations and comprehensive analysis have evaluated the performance and revealed that the scheme can effectively secure the sink location with satisfied energy consumption and delivery time compared with others. In the future, the work will be extended to enhance sink privacy with multiple path segments in mobility control.

Acknowledgement: This work is funded by a grant from the Long-Term National Plan for Science, Technology and Innovation (LT-NPSTI), No. 11-INF1702-10, the King Abdulaziz City for Science and Technology (KACST), Kingdom of Saudi Arabia. We thank the Science and Technology Unit at Umm A-Qura University for their continued logistics support.

7. References

[1] Ananthram Swami, Qing Zhao, Yao-Win Hong and Lang Tong Wireless Sensor Networks Signal Processing and Communications Perspectives, John Wiley&Sons, England, 2007.

[2] Feng Zhao and Leonidas J. Guibas , Wireless Sensor Networks: An Information Processing Approach, Elsevier, California, ISNB: 978-155860914-3, Ch. 1, 2004

[3] Nor Azlina Ab. Aziz, Kamarulzaman Ab. Aziz, and Wan Zakiah Wan Ismail "Coverage Strategies for Wireless Sensor Networks", World Acad. of Sci., Eng. and Tech., Vol. 50, pp. 145-150, 2009.

[4] Chee-Yee Cong and Srikanta P. Kumar,"Sensor Networks: Evolution, Opportunities, and Challenges", Proc. IEEE, Vol. 91, pp. 1247-1256, 2003.

[5] Peter Csaba Ölveczky and Stian Thorvaldsen, "Formal modeling, performance estimation, and model checking of wireless sensor network algorithms in Real-Time Maude", Theoretical Computer Sci., Vol. 410, pp. 254-280, 2009.

[6] Lin Yao et al., "Protecting the sink location privacy in wireless sensor networks", Pers Ubiquit Comput Vol. 17, pp. (883–893)2013.

[7] Yun Li, Leron Lightfoot, Jian Ren, "Routing-based source-location privacy protection in wireless sensor networks", Electro/Information Technology, 2009. eit '09. IEEE International Conference on, pp. (29 – 34), 2009.

[8] Basavarajeshwari, Jitendranath Mungara and Manimozhi Iyer, "Mitigating Hotspot Locating Attack in Wireless Sensor Network", International Journal of Science and Research (IJSR), India, Volume 2 Issue 6, pp.(366-371), 2013.

[9] Revati A. Parate , Pragati Patil and Girish Agarwal, "Survey On Location Privacy Preserving Schemes In Wireless Sensor Network", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 9, pp. (1-5), 2012.

[10] Rini Van Solingen and K. Janani, "Securing the Location Privacy in wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1,pp. (1-4), 2013.

[11] Ying Jian et al., "Protecting Receiver-Location Privacy in Wireless Sensor Networks", INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pp. (1955-1963), 2007.

[12] Zhenhua Liu and Wenyuan Xu, "Determining sink location through Zeroing-In attackers in wireless sensor networks", Wireless Networks, Vol. 18, Issue 3, pp 335-349, 2012.

[13] Bidi Ying, Jose R. Gallardo, Dimitrios Makrakis, Hussein T. Mouftah1, "Concealing of the Sink Location in WSNs by artificially homogenizing traffic intensity", The First International Workshop on Security in Computers, Networking and Communications, pp. (988-993), 2011.

[14] Jing Deng, Richard Han and Shivakant Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks", in Security and Privacy for Emerging Areas in Communications Networks(SecureComm'05), 2005.

[15] Xinfeng Li et al., "Enhanced Location Privacy Protection of Base Station in Wireless Sensor Networks", Mobile Ad-hoc and Sensor Networks, 2009. MSN '09. 5th International Conference on, pp. (457 – 464), 2009.

[16] Patil Ganesh G and Madhumita A Chatterjee, "Selective Encryption Algorithm for Wireless Ad-hoc Networks", IJACTE, Vol.1, Issue 1, pp.35-38, 2012.

[17] Taochun Wang, Xiaolin Qin and Liang Liu, "An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks", International Journal of Distributed Sensor Networks Vol. 2013, pp. 1-11, 2013.

[18] Sajad Rahmdel, Ma Bairamai, and M. Mansoorzadeh Hamid Reza Fahham, "Design Chattering-Free Performance-Based Fuzzy Sliding Mode Controller for Bus Suspension", International Journal of Engineering Sciences Research-IJESR, Vol. 03, Issue 05, pp. 796-802, 2012.

[19] Erin-Ee-Lin Lau, Boon-Giin, and Seung-Chul Lee Lee. "Wan-Young Chung,"Enhanced RSSI-Based High Accuracy Real-Time User Location Tracking System for Indoor and Outdoor Environments,"." International Journal on Smart Sensing and Intelligent Systems 1.2 (2008).

[20] Georgios Smaragdakis, Ibrahim Matta and Azer Bestavros, "SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks", 2004.