I.J. Information Technology and Computer Science, **2016, 10, 22-28**
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.10.03

Witness-Header and Next-Node Selection to Extend Network Lifetime in Energy-Efficient Clone-Node Detection in WSNs

Muhammad K. Shahzad and Quang-Ngoc Phung
College of Information and Communication Engineering, Sungkyunkwan University,
Suwon 440-746, Republic of Korea
E-mail: {khuram, ngocpq}@skku.edu

Abstract—Wireless sensor network (WSN) has emerged as potential technology for their applications in battlefields, infrastructure building, traffic surveillance, habitat monitoring, health, and smart homes. Unattended nature of these networks makes them vulnerable to variety of attacks, the inherent stringent resources makes conventional security measure infeasible. An attacker can capture a sensor node to install number of clone nodes with same privacy information causing serious security threats and deterioration in network lifetime. Current, security scheme along with distinct advantages suffer from number of limitations. A good counter attacks measure should not only cater for security and energy-efficiency but network lifetime as well. In this paper, we propose a next-node selection method which consider residual energy and clone attacks ratio in addition to distance, in order to overcome the limitation of fixed path based shortest routing. These factors are also considered while selecting the witness header in WSNs. Results demonstrate the efficacy of the proposed schemes in terms of network lifetime.

Index Terms—Wireless sensor network, Network protocols, network lifetime, dynamic routing, next node, and witness header selection.

I. Introduction

Wireless sensor networks (WSNs) have emerged as promising technologies for numerous applications in civil and military. Secure communication is one of the most challenging and risky tasks. WSNs are found to be prone to clone node attacks that effects in many harmful ways. In a clone node attack, an adversary captures a node and installs its code with same privacy information. Later adversary makes multiple copies of the node and installs them throughout the network to take control of the network. If these clone nodes are not detected, network is left vulnerable to attacks and thus severe damage. A typical clone node attack scenario is shown in Fig. 1.

To counter these attacks security measures have been proposed [1-7]. Most of the methods focus on having high detection ratio of these attacks without network lifetime being of major concern. In research [1], authors presented an energy efficient clone detection (ERCD) protocol which also shows improvements in network lifetime. This scheme however, also have some limitations; it consider transmission energy but ignores receiver energy consumption, it is based on distance based routing which is based on fixed paths, and it may not work if witness header is dead or compromised among other. We counter these limitations in our proposed method and further improve network lifetime.

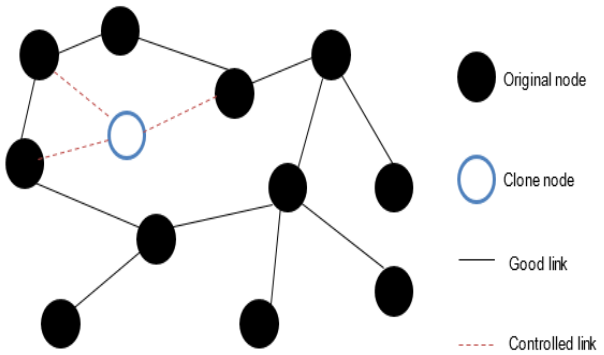

Fig.1. A Clone Attack Scenario

In order to balance network energy consumption, next-hop nodes for routing and filtering nodes should be dynamically selected. The inputs of the model are energy level, number of hops, and false traffic ratio (FTR). This next hop selection method is used for forwarding node selection in the underlying routing and witness header selection. The original scheme is based on shortest path routing which consider only distance for selecting next hop forwarding node which is fixed path routing in essence. Our scheme can dynamically opt for different paths based on current energy levels of the candidate nodes. Similarly, for verification or witness node selection, if the fitness value of a node is higher among candidate nodes than it will be witness node with filtering false report capabilities. This will help balancing network wide energy usage and thus prolong the network lifetime.

In ERCD, the witness header is bottle neck of the scheme, since after a witness header of a witness ring energy level reaches to zero or compromised, it could not work. In our proposed method at the cost of multiple witness header management instead of single one, the

verification traffic load balance distributed. This load distribution along with next hope selection method results in more balanced energy consumption approach. Clone node detection or energy-efficiency are not focus of this paper. We proposed energy-aware dynamic routing, next hope, and witness header selection to more evenly distribute the communication loads to further extend the network lifetime. Following are the expected contributions of our proposed method as compared to ERCD.

- Network lifetime improvements
- Dynamic path selection
- Traffic load balancing with multiple witness header

The rest of the paper is organized as follows; Section 2 presents an overview of the related work, section 3 shows the system assumptions and system model, the detail of our proposed method is explained in the section 4, numerical results based on the analysis and simulation is illustrated in section 5, and conclusion and future work at the end of this paper.

II. Literature Review

Wireless sensor networks [WSNs] have become very popular and ubiquitous technologies for everyday applications. However, there a number of challenges to be addressed for secure communication. WSNs are vulnerable to clone node attacks that effects in many devastating ways. To counter these attacks security measures have been proposed [1-7]. Most of the methods focus on having high detection ratio of these attacks without further improving and network lifetime as main concern.

In energy-efficient clone node detection (ERCD) protocol in WSNs [1], a location based, clone node detection protocol has been presented. It can grantees clone node detection and have minimal effect on network lifetime. Witness node used in verification of privacy information is randomly selected from a ring area to detect these attacks. Ring structure is used for energy-efficient data forwarding towards the witness node, witness header, and sink or base station (BS). This distributes the load balance within the network and help in improving network lifetime. Analytical and simulation results show the efficacy of proposed method which can achieve up to 100% detection with trustful witnesses. The proposed scheme further studies clone node detection with untruthful witness. With presence of 10% compromised witnesses detection probability can approach up to 98%.

In work [2], a centralized SET approach based on set operations is proposed. It tries to limit detection overhead by computation of set operations of union and intersection of exclusive subsets in the sensor network. SET scheme divide the network into logically separate and non-overlapping regions or clusters controlled by a cluster head (CH). These CHs send reports to BS containing IDs of all nodes in its cluster and itself in the form of a subset. The set operations are performed after computing the subsets. If the intersection of any two subsets if non-empty set a clone attack is detected.

The work [3], presents a survey of clone node attacks in WSN. An attacker can physically capture a node and duplicated one or more nodes at strategic locations to control and damage the entire network. The authors study variety of threats specific to clone node attacks and analyses different detection schemes and classify them in different categories. It comprehensively explores different proposals in each category. The discussed schemes are evaluated and there advantages and limitations are highlighted.

In research [4], proposes two novel clone node detection schemes. First scheme is distributed hash tables (DTH) and second one is randomly detected exploration (RDE) scheme. The simulations results verify the protocol design and demonstrate its efficiency in communication overhead and satisfactory detection probability.

Recent clone detection schemes such as randomized efficient and distributed (RED) [5] and line-select multicast (LSM) protocol [7], fail to guarantee both requirements of use random witnesses selection and a significant probability of clone detection. For example; RED protocol attains a high clone detection rate with the assistance of deterministic mapping function in witness selection. Since, a deterministic mapping function is also probable to be compromised, and compromises on randomness of selection of witness nodes which degrades security. However, in LSM protocol, a source node can randomly select multiple sink nodes and establish paths to those nodes. If a witness node obtains several copies of verification messages from the single source along various paths, it identify it a clone attack which triggers a revocation procedure. LSM results in a low detection probability in case of a small number of witnesses. This is because the intersection of multiple paths should a witness node which probability is dependent on density of witness nodes.

In [6], authors focus on solving the critical problems of energy and memory. In order to solve these problems a fast, lightweight, efficient, and mobile agent based security scheme has been proposed against clone node or replicating node attacks. Mobile agents are software defined which require minimum energy usage by nodes. These agent can also cooperate with the outside world for collaboration and self-governing. In [7], a distributed algorithm for clone node detection is presented. The paper focusses the effect of undetected clone nodes and their effect on communication overhead and storage cost incurred by each algorithm. An optimization framework has been proposed for selection of clone node detection parameters based on above mentioned cost analysis. Simulations are provided to validate the framework.

In this paper, energy dissipation model or first order radio model [8, 9] is used to compare the energy consumption of ERCD and our proposed protocol. A typical sensor node composed of a data processing unit, a

micro sensor unit, antenna, radio communication components, power supply, and amplifier. In our implementation of the first order radio model, we only consider the energy usage that is associated with the radio component. Moreover, the clocks of the sensor nodes assumed to be synchronized using an energy-efficient time synchronization protocol(ETSP) in WSNs [10].

In research [11] two clone node detection schemes based on hash table value and probabilistic directed diffusion are presented using NS2 simulator. The authors [12] on general network deployment graph presented distributed hash table based clone detection scheme. Secure routing scheme was presented [13] by secure directed diffusion protocol. Work [14], presented a security scheme for wormhole detection at MAC layer in WSNs. The authors in [15], proposed quality of service improvement scheme in WSNs based on symmetric key cryptography schemes.

III. System Assumptions and Models

A. System Assumptions

Some localization component is assume to present in the system so that after random deployed each sensor node knows its location. This is necessary because, after an event is spotted, its location is required to create the path in order to report the event to the BS. After sensor nodes are deployed, the boot-up process is started with a localization component.

We also assume bidirectional communication links in the sense that both source and sink can send and receive the messages. Each node also possesses a unique ID and also knows its key. Each node has at least one witness nodes which know the privacy information of the original node. Each witness ring has one witness header. All the sensor nodes have a limited and fixed sensing range and contains a battery with a limited and fixed initial energy of 1 Joule.

B. Experimental Setup Model

In this paper, we consider a 2000-node randomly distributed sensor network. The simulation has been performed in custom built simulator in Microsoft Visual Studio 2012 using C#. This network is based on ring based topology. The stated network has an area of πr2 m2 with k ring based clusters. The sensor nodes are distributed in s sectors of the sensor network. All the sensor nodes has a range R which is used to determine neighbors and candidate nodes. The BS is stationary and knows the node IDs and their locations in advance. The sensor field setup used performance analysis is shown in Fig. 2.

Table I presents the simulation parameters for the performance analysis in experimental setup.

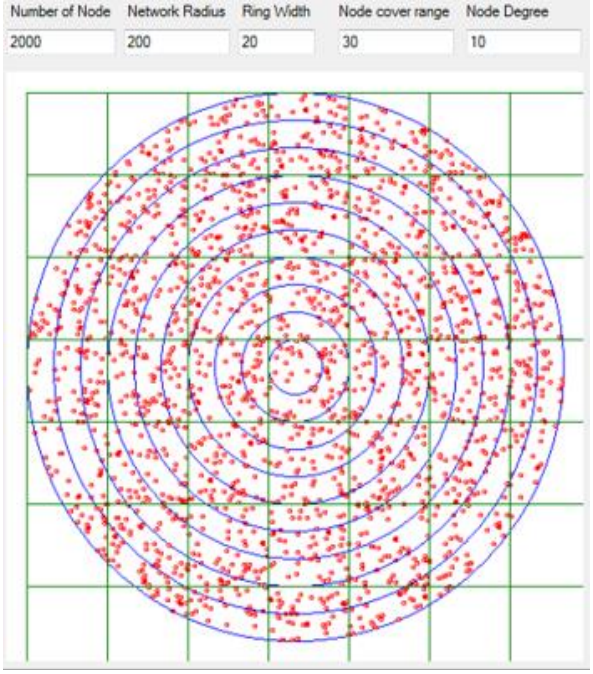

Fig.2. Randomly Deployed Circular Sensor Field.

Table 1. Simulation Experiment Parameters

Parameter	Value
Number of nodes	2000
Sensor field radius	r=200
Field size	πr2 m2
Base station location	Ring center
Node Range	30 m
E_{elec}	50 nJ/bit
E_{amp}	100 pJ/bit/m2
Initial node energy	1 Joule
Packet size	200 bits
Path loss constant (λ)	2

C. First Order Radio Model

In this paper, first order radio model or energy dissipation model in [8, 9] is used compare the energy-efficiency performance of ERCD and proposed method. A sensor node composed of a radio components, data processing unit, antenna, power supply, a micro sensor unit, and amplifier.

In this paper, we only consider the energy consumption that is related to the radio components. A classic, simple, and most utilized energy consumption analysis model is the first-order radio model illustrated in Fig. 3.

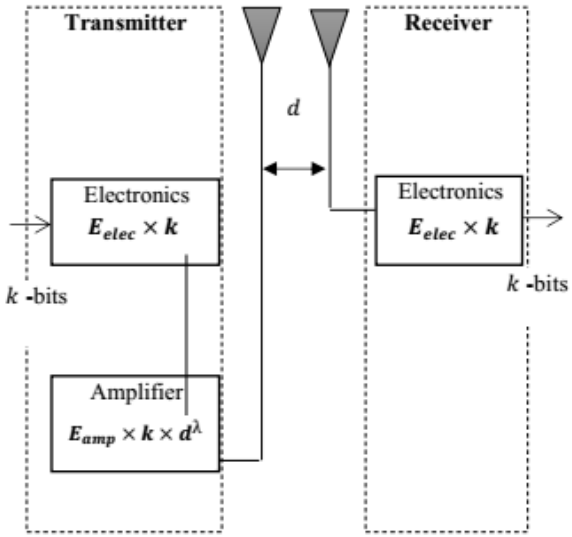

Fig.3. The First-Order Radio Model.

For transferring k-bit packet over a distance d between the transmitter and receiver, the transmission energy $E_{T_x}(k, d)$ is represented by Eq. (1):

$$E_{T_x}(k, d) = E_{elec} \times k + E_{amp} \times k \times d^{\lambda} \quad (1)$$

Where E_{elec} is the energy consumed by the electronics of the circuitry, $E_{elec} \times k$ is the energy utilized by the transmitter electronics to transfer k bits, E_{amp} is the energy needed by the amplifier, and λ is the path loss constant. Similarly, $E_{R_x}(k)$ is the energy required to receive k bits:

$$E_{R_x}(k) = E_{elec} \times k \quad (2)$$

IV. Proposed Method Overview

In this section we explain the overview of the proposed method.

A. Network Initialization

In setup phase all nodes IDs and location information is pre-loaded on every node. BS also knows the location and ids and all sensor nodes in the network. Initialization phase and BS are assumed to be secure.

B. Neighbour and Witness Discovery

Assuming the location component, every node determines its neighbors' information and distance. This location information is broadcasted to neighbors. Using breadth first search (BFS) the location of the witness header is obtained.

C. Next Node Selection

After an event is detected, the event discovering nodes send reports to the BS. A path is created using an evaluation function which considers energy level and distance of neighbor nodes to select forwarding node among candidate nodes. A node with highest energy and closer to the destination will be selected to forward the report. This process will continue until destination is reached.

D. Witness Selection

A source node A randomly generates witness index for node B. Wi is ring index (Ri) of the witness. Then this node will create a witness node selection message and send it to the node B. After node B received the message node B record the privacy information of the node A which sends a broadcast message to all it neighbors so announce that it is witness node of A. If node A cannot find the witness node in Wi of node B ring than node B forwards witness selection message to farthest left neighbor of it in the witness index ring (Ri). This will continue until witness selection procedure is finished. This process is explained the flow chart presented in Fig. 4.

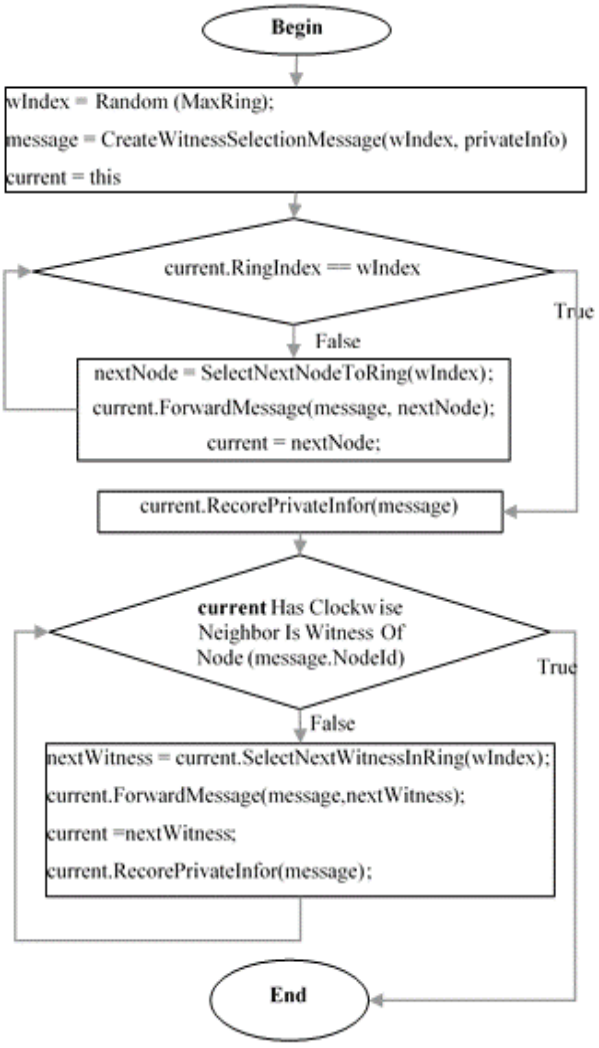

Fig.4. Witness Selection Phase.

E. Message Verification

When a node has data to transmit to the BS, it create a data message, it will send the message to three rings Ri-1, Ri, and Ri+1. After a node in these rings receives a

message, if there is no witness node in its ring the message is dropped. In that case message will be forwarded to one of its neighbors that is witness of node A. When a witness of node A, i.e. Aw, receives data message it will check number of conditions for verification of the message. In case witness header is one of its neighbors than data message should be forwarded to it. A number of verification conditions should be met before witness header forward message to BS.

- Witness header will check sender ID and location information, if this matches with the values at witness header
- In case of receiving multiple copies of the message with same privacy information
- If the time stamp of the received message is earlier or equal to the last data message generated drop the message. If not the time stamp for the last message received is updated.

If all the conditions are met the message will be forwarded to BS otherwise clone node is detected and revocation message is generated. The pseudo code for the verification process is shown in the Fig. 5.

Step: 1. NodeA create a DataMessage ***msg***
Step: 2. Node send the message to it witness ring (ring index is wIndex) and two neighbor ring of the witness ring (ring indexes is wIndex-1 and wIndex +1).
Let node1, node2 and node3 is three nodes in the three rings have received message.
Step: 3. Foreach Node **N** in {node1, node2, node3}
If there is no witness of ***NodeA*** in node n's neighbors *then*
The ***msg*** will be drop.
Else Select a witness node ***W*** is one of its neighbors that are the witness of **NodeA**.
Forward the ***msg*** to ***W***
The next step is described in Step 4, when the message comes to node **W.**
Step: 4. When a witness of nodeA, called **W**, receives the DataMessage.
If the creation time of the ***msg*** <= the creation time of the last DataMessage it received from **nodeA** then drop.
Else Node **W** update ***the last msg time*** in its memory
If ***witness header*** *is one of its* ***neighbors*** then
Forward the ***msg*** to the WitnessHeader
The next step is describe in Step4, when the WitnessHeader receive message
Else Node**W** forwards the message to a next neighbor that is a witness of nodeA and in the direction to the witness header (**WH**).
Step: 5. **WH** verify ***msg*** and then forward to the BS if it valid.

Fig.5. Message verification (NodeA sending msg to BS)

V. Numerical Analysis and Results

In this section, we give two examples to elaborate better expected performance of our algorithm in section 5.1 and simulation experiments of network lifetime performance results in section 5.2 of this paper.

A. Numerical Analysis

In order to explain how our proposed method will be able to increase network lifetime, let's consider an example scenario. In original scheme network lifetime is define as number of events before the first node is depleted due to running out of battery power. Since, verification takes place on witness header node, so most of the energy will be consumed at this node. The lifetime of the network will depend upon how long it will take for the first witness header to be depleted in ERCD. In our proposed scheme in addition to using different path dynamically based on remaining energy we have multiple witness headers. Consider one example of next node selection method and another with multiple witness headers.

Example 1: Next node selection (Fixed vs Dynamic)

Since, ERCD is based on shortest path distance based routing, it will use the same path until some node is depleted which forces it to create or use another path. Let's consider a scenario where there are three existing paths amount source and sink nodes. In case of our proposed method since current energy level is also considered, based on current energy level, one of these three paths will be used alternatively. This will balance the energy usage upon nodes on three paths. This will result in communication of more events before first of nodes in three paths is depleted. ERCD will use path 2 before first node is depleted. ERCD will use path 2 since this is shorted path with next node closest to the BS. However, in case of our proposed scheme if only half messages are communicated to sink using path 1 and path 3, network lifetime will improve twice as compared to ERCD. This scenario is illustrated in Fig. 6.

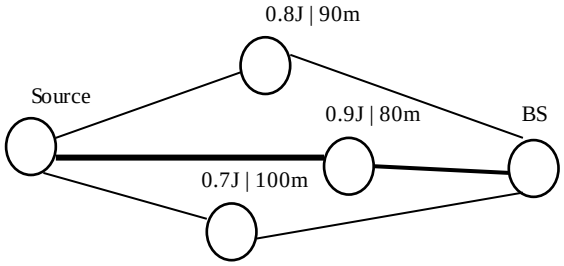

Fig.6. Example 1 - Next node selection example.

Example 2: Multiple witness headers (One vs Multiple)

In previous example; different paths can be used to distribute the energy usage to extend network lifetime. However, since most of the energy will be consumed by the witness header this will result in bottleneck. So, in order to cater for this problem, we introduce multiple witness headers to further distribute the energy usage and achieve load balancing. Since, verification can be performed alternatively or another witness header among three is used after one energy level drops to threshold, our proposed scheme will balance the network energy usage in a better way. Although, there is some cost associated with managing of three witness headers instead of one,

however, this cost is justified by the gain in network lifetime. This scenario is highlighted in Fig. 7. ERCD will use shortest path through witness header 2 as highlighted with bold line. However, our proposed scheme, both witness headers can receive messages for verification to divide verification frequency overhead and thus by balancing the network energy usage we can extend the network lifetime and avoid the bottleneck.

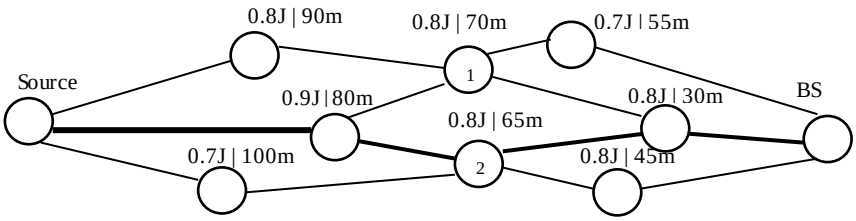

Fig.7. Example 2 - Multiple witness headers example.

B. Results

The simulation experiments are performed in the custom simulator in Microsoft Visual Studio 2012 in C# is shown in the Fig. 8. We perform the network lifetime analysis of the two methods in this section.

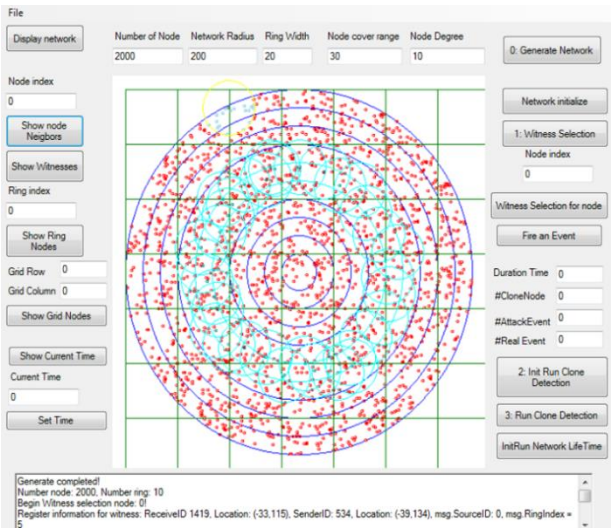

Fig.8. Simulator - Node id 0 (Center of the yellow cycle), and the witness ring (Cyan cycles)

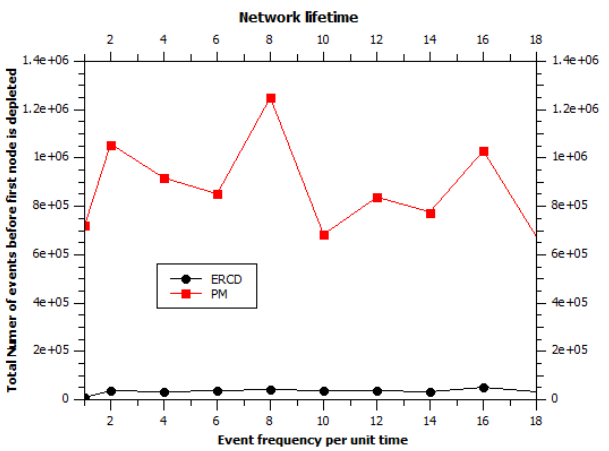

Fig.9. Network lifetime against different initial frequencies of events.

In the Fig. 9, the comparison of network lifetime of ERCD and proposed method (PM) is presented. We define network lifetime as number of events before first node is depleted. Figure shows frequency of events generation on x-axis and number of events before first node depleted at y-axis. Figure demonstrates the validity of our method to extend the network lifetime.

The network lifetime perform of two methods with different initial battery a level in Joules is shown in the Fig. 10. Our proposed method performs significantly better than ERCD method in order to prolong the network lifetime. The results are due to the next node selection method which is able to balance the energy utilized throughout the sensor network better than ERCD.

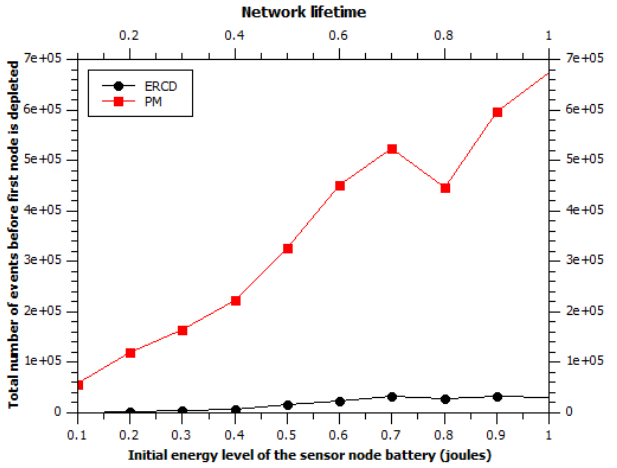

Fig.10. Network lifetime with different initial sensor battery levels.

VI. Conclusions and Future Work

In this paper, we have shown that our proposed scheme has multiple advantages; network lifetime improvements, dynamic path selection, and traffic load balancing with multiple witness headers. These factors results in better network energy usage balance to prolong the network lifetime. In current work we have implemented the network lifetime analysis. In future work, we would like to implement the clone node detection to test the energy-efficiency and detection capacity performance of our approach.

REFERENCES

[1] Zhongming Zheng, Anfeng Liu, Lin X. Cai, Zhigang Chen, and Xuemin (Sherman) Shen, "ERCD: An Energy-Efficient Clone Detection Protocol in WSNs," Proceedings of IEEE INFOCOM, pp. 2436-2444, 2013.

[2] Heesook Choi, Sencun Zhu, Thomas F. La Porta, "SET: Detecting node clones in Sensor Networks," Third International Conference on Security and Privacy in Communication Networks, SecureComm, pp. 341-350, 2007.

[3] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey," pp. 1-22, vol. 2013, 2013.

[4] Zhijun Li, Member and Guang Gong, "On the Node Clone Detection in Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, pp. 1799-1811, vol. 21, no. 6, December 2013

[5] Bryan Parno, Adrian Perrig and Virgil Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," IEEE Symposium on Security and Privacy, pp. 49-63, 2005

[6] R.Sathish, and D.Rajesh Kumar, "Dynamic Detection of Clone Attack in Wireless Sensor Networks," International Conference on Communication Systems and Network Technologies, IEEE Computer Society, pp. 501-505, 2013

[7] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, pp. 685-698, vol. 8, no. 5, SEPTEMBER/OCTOBER 2011

[8] Swarup Kumar Mitra, Mrinal Kanti Naskar, "Comparative Study of Radio Models for data Gathering in Wireless Sensor Network," International Journal of Computer Applications (0975 – 8887), Volume 27– No.4, pp. 49-57, August 2011

[9] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Sensor Networks,"Proceedings of the Hawaii International Conference on System Sciences, January 4-7, 2000.

[10] Shahzad, Khurram; Ali, Arshad; Gohar, N. D., ETSP: An Energy-efficient Time Synchronization Protocol on Wireless Sensor Networks. (2008). IEEE 22nd International Conference on Advanced Information Networking and Applications (22ndIEEE AINA), Okinawa, Japan.

[11] Neenu George, T.K.Parani, "Detection of Node Clones in Wireless Sensor Network Using Detection Protocols," IJETT, vol.8, no.6, pp.286-291, 2014. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group.

[12] Zhijun Li, Guang Gong, "DHT-Based Detection of Node Clone in Wireless Sensor Networks," Ad Hoc Networks, LNICST 28. ISBN 978-3-642-11722-0. Springer Berlin Heidelberg, p. 240-255, 2010.

[13] Malika BELKADI, Rachida AOUDJIT, Mehammed DAOUI, Mustapha LALAM, "Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks", IJITCS, vol.6, no.1, pp.50-56, 2014. DOI: 10.5815/ijitcs.2014.01.06

[14] Louazani Ahmed, Sekhri Larbi, Kechar Bouabdellah,"A Security Scheme against Wormhole Attack in MAC Layer for Delay Sensitive Wireless Sensor Networks", IJITCS, vol.6, no.12, pp.1-10, 2014. DOI: 10.5815/ijitcs.2014.12.01

[15] Er. Gurjot Singh, Er. Sandeep Kaur Dhanda,"Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes", IJITCS, vol.6, no.8, pp.32-42, 2014. DOI: 10.5815/ijitcs.2014.08.05

Authors' Profiles

Muhammad K. Shahzad received a B.E.I.T degree from the University of Lahore and an M.S. degree in Information Technology from the National University of Science and Technology, Isalamabad, Pakistan in 2004 and 2007, respectively. He is now a Ph.D. scholar in the College of Information and Communication Engineering at Sungkyunkwan University, South Korea. His research interests include wireless sensor networks and graph gheory.

Quang-Ngoc Phung received the BEng degree in IT from the University of Technology and Education, and the M.S. degree in Computer Science from the University of Science, Ho Chi Minh city, Vietnam in 2008 and 2013, respectively. He is now a Ph.D. scholar in the College of Information and Communication Engineering at Sungkyunkwan University, South Korea. His research interests include Self-Adaptive Software System, and Automatic Software Engineering.

How to cite this paper: Muhammad K. Shahzad, Quang-Ngoc Phung, "Witness-Header and Next-Node Selection to Extend Network Lifetime in Energy-Efficient Clone-Node Detection in WSNs", International Journal of Information Technology and Computer Science (IJITCS), Vol.8, No.10, pp.22-28, 2016. DOI: 10.5815/ijitcs.2016.10.03