Vol. 1, No. 1 | Jan – June 2017

Increasing the Energy Efficiency of TICK by Selecting Adaptive Forwarding Nodes in Wireless Sensor Networks

Muhammad Ashraf, Muhammad Akram
College of Information and Communication Engineering, Sungkyunkwan University, Suwon 16419, Republic of Korea
ashraf84@skku.edu , akram.khan@skku.edu

Tae Ho Cho
College of Software, Sungkyunkwan University, Suwon 16419, Republic of Korea
thcho@skku.edu

Abstract

Time-Based Dynamic Keying and En Route Filtering (TICK) reduces the communication costs for wireless sensor networks by eliminating the exchange of control keying messages. TICK is more energy-efficient and is good at securing events as they occur; it also selects predetermined forwarding nodes for re-encryption operation without considering their residual energy (RE) which causes more energy depletion. We propose an energy- efficient method that selects forwarding nodes for re-encryption with high energy levels and a low hop count (HC). Simulation results indicate that the proposed method achieves better energy conservation.

Keywords: Wireless sensor networks; SNs; network energy; en route filtering

1. Introduction

Modern technological advancements have led to the development of sensor nodes. Each sensor node has a constrained data processing capability, restricted storage, low-powered resources, and a small communication area. Still, they have the potential to thoroughly monitor a given physical environment. A collection of such nodes is called a sensor network and can be used in various applications, including health, transportation vehicles and intelligent highways [1]. Since sensor nodes are left unattended and are deployed in a hostile environment without any infrastructure, adversaries can easily compromise these nodes [2, 3]. In addition, sensor nodes carry limited and generally irreplaceable power sources. Therefore, providing energy efficiency and resilience against false injected data are the most important factors.

The TICK scheme [4] addresses these issues and minimizes the communication costs. It is also resistant against false information being injected into sensor-based applications via a novel approach. TICK achieves high energy savings by eliminating the exchange of control messages regarding keying or rekeying. We propose a method that efficiently selects forwarding nodes for re-encryption operation by considering the residual energy (RE) of the forwarding nodes, along with their hop count (HC); this determines which forwarding nodes are more suitable for re-encryption operations in order to reduce the risk of classifying a valid message as malicious and increase the energy efficiency of forwarding nodes.

The proposed method presents the following contributions:

- Reduced false positive classification.
- Improved energy efficiency by selecting en route nodes with high energy level.

The rest of this paper is organized as follows: Section 2 presents related work. A comprehensive description of the proposed method is provided in Section 3. A performance evaluation of the proposed method is discussed in Section 4 and conclusion is presented in Section 5.

2. Related Work

Many en route filtering schemes have been developed that filter malicious data from the wireless sensor networks (WSNs). In Dynamic En route Filtering (DEF) [5], several nodes employ their authentication keys to endorse legitimate reports. Hence, it depletes more energy via authentication and by using separate secret keys. In Statistical En route Filtering (SEF) [6], different keyed Message Authentication Codes (MACs) are used to validate each sensed report. In this way, the size of the reports increases due to the MACs overhead. Although bloom filters are helpful in decreasing the overhead of MACs, they have many flaws implemented in static key management schemes.

The Bandwidth Efficient Cooperative Authentication for Sensor Networks (BECAN) [7] scheme is based on the graph characteristics of node deployment and the cooperative bit-compressed authentication technique. It provides high security by early detection of injected false data in the network but causes extra-overhead at the forwarding nodes and consumes unnecessary energy resources due to the multi-report solution. Selcuk et al. [1] presented a TICK scheme for WSNs that sends reports to the base station without sending rekeying messages. Sensor nodes encrypt each report with a dynamic key generated by their local time values. The working principle of TICK protocol is comprised of three phases. In the first phase, when an event occurs, the source node utilizes its local time variable and generates a one-time dynamic key. The dynamic key is a function of the source node's local time (t_1) and the initialization vector (IV), as shown in equation (1)

$$K_1^t = F(t_l + IV) \tag{1}$$

The initialization vector is loaded in every node at the time of deployment. The generated one-time dynamic key is then used for security services such as encryption and authentication. Finally, the encrypted report is sent to the upstream forwarding nodes.

Although TICK saves more energy compared to other schemes like DEF, SEF, and BECAN, it selects forwarding nodes for re-encryption ineffectively, causing rapid depletion of the limited energy resources. This strategy is pre-determined that every 3rd, 5th, or 7th forwarding node is selected for the re-encryption operation while trying to maintain the time window bound, as shown in *Fig.1*. The problem with this strategy is that it does not consider the residual energy of en route nodes and the selected forwarding nodes are fixed and dedicated for the re-encryption operation. These selected nodes must continuously perform re-encryption operation, which depletes more energy and may die early.

3. PROPOSED METHOD

A. Overview

The proposed method utilizes the functioning modules of TICK and modifies the crypto (CRYPT) module. The other two types of modules, i.e., time-based key management (TKM) and filtering-forwarding (FFWD) modules, are the same as in equation 1.

B. Crypto (CRYPT) Module

This module obtains the dynamic key generated at the TKM module and performs the required security operations. The key from the TKM module is also verified in this module. If the verified key is not correct, it obtains another key from the TKM and continues this operation until it finds the correct key. Otherwise, it considers the report as malicious and drops it in the FFWD module when all attempts to find the correct key are exhausted within the tick window (TW).

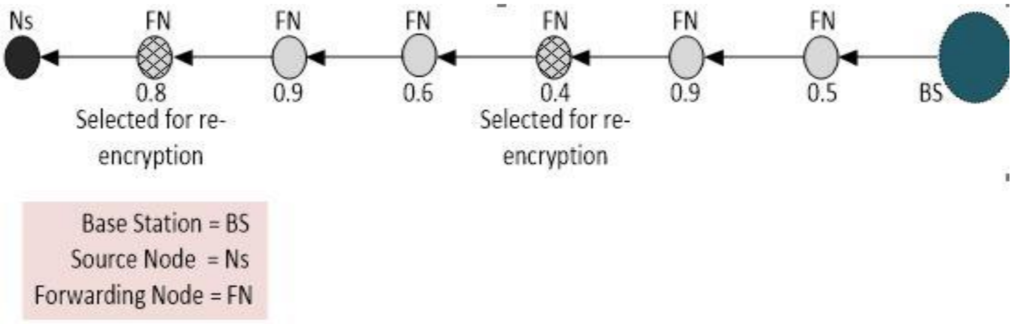

Figure. 1: Selection of Forwarding Nodes in TICK

In our proposed method, we employ a selective re-encryption operation in the CRYPT module, reducing the chances of considering a safe incoming report as malicious and conserving the energy of the forwarding nodes as much as possible. The BS regularly monitors the network status after a session of traversing reports expires. The BS decides which nodes are to be selected for the re-encryption based on two parameters (RE and HC), as shown in *Fig. 2.*

We have considered remaining energy of the node because in each round there will be some energy consumption at each node. So, after processing each round, the remaining energy is considered for the next round. If the RE of the forwarding node is less than the threshold, the node is discarded from consideration for selection for re-encryption in order to extend the battery life of the node.

$$\mathrm{RE} = \mathrm{E}_{\mathrm{Ni}} > \mathrm{TH} \tag{2}$$

Selection of the forwarding node for re-encryption is based on its energy state being greater than the threshold:

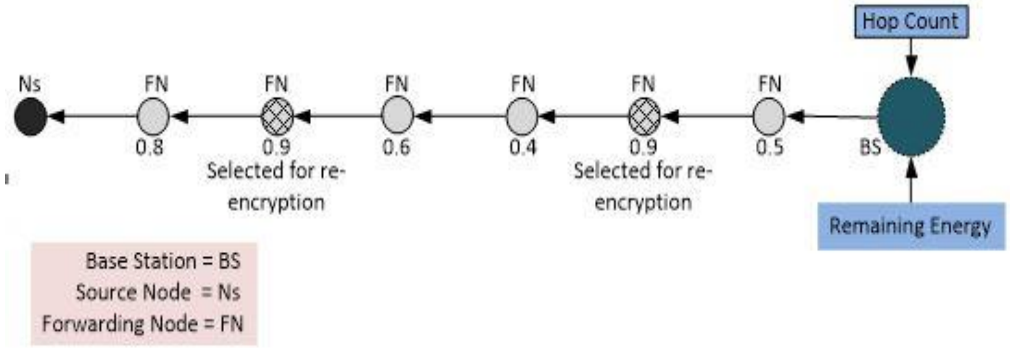

Figure. 2: Selection of Forwarding Nodes in the Proposed Method

Here, E_{Ni} is the current energy of ith node and TH is the threshold.

The hop count (HC) is another vital factor in selecting forwarding nodes for re-encryption. HC in our work is the distance between two sensor nodes that are capable of performing re-encryption. If the distance between two encrypting nodes increases, the safe report

$$HC = d_1 - d_0 < TW \qquad (3)$$

May be dropped by classifying it as a malicious report. Our proposed method considers this factor and selects the forwarding nodes for re-encryption depending on the HC status. If the HC between source node and receipt node is within the time window (T_w), the node is selected for selection for re-encryption, otherwise, the candidate node is discarded from the competition. The HC is computed as:

Here, d_1 is distance of candidate en route node, d_0 is the distance of source node and TW is the time window.

4. Performance Evaluation

A. Simulation Parameters and Assumptions.We have simulated the proposed method in a custom simulator developed in Microsoft Visual C ++ 2010. Network details and parameters are presented in Table 1.

The network is composed of a BS and 500 sensor nodes; the nodes are randomly deployed in a field of size 100 m × 100 m. The BS is located at the edge of the network and knows the sensor nodes' IDs and their location information in advance. The sensor network used in our method is shown in *Fig.3.* Each sensor node has a fixed and limited sensing range and is battery powered with a fixed limited energy of 50 mJ. In order to achieve an energy efficient network, it is essential to consider the residual energy of all candidate nodes in order to select the forwarding node. This helps improve the energy efficiency by selecting the number of participating nodes with high energy levels.

Table 1: Simulation Parameters

Parameter	***Value***	***Parameter***	***Value***
No. of nodes	100	E_{ini}	50 mj
Network size	100 * 100 m^2	E_{rx}	66.7 µj
BS location	0 * 0 m^2	E_{tx}	59.6 µj
Link rate	250 kbps	E_{sens}	9.0 µj
Range	30 m	E_{enc}	3.3 µj
Report size	28 Byte	E_{dec}	3.3 µj
Tick window	16	E_{mac}	8.6 µj
Time offset	U [-3, +3] µs		

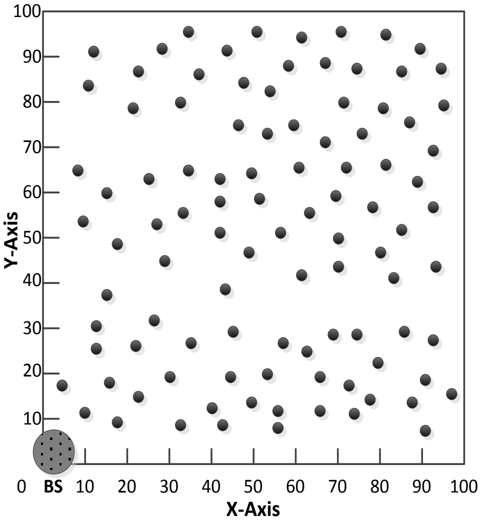

Figure. 3: Random Deployment of Sensor Nodes in the Network

A. Simulation Results

The source node generates reports and sends these reports to the BS. The proposed method achieves high energy savings compared to the target method, and *Fig. 4* shows the energy consumption of selected forwarding (re-encrypting) nodes versus the number of rounds. This shows that the proposed method efficiently selects dynamic forwarding nodes for the re-encryption operation by considering the two main factors (REL and HC). However, this is not the case in the target method, where the forwarding nodes for re-encryption are pre-decided. These nodes have to perform the re-encryption operation continuously, and, in turn, they will consume more energy as the number of data rounds increases.

As selected forwarding nodes are pre-decided based on each 3rd node strategy in the target method, and does not consider the residual energy of en route nodes. So, the selected forwarding nodes will deplete more energy, as they have to continuously perform re-encryption and may eventually die. Some reports generated by the source node do not reach the BS, as some of the forwarding nodes die earlier due to continuously performing the re-encryption operation; this information cut-off point is reached earlier in the target method than for the proposed method. Hence the proposed method extends the network lifetime. The number of depleted nodes is shown in Fig. 5.

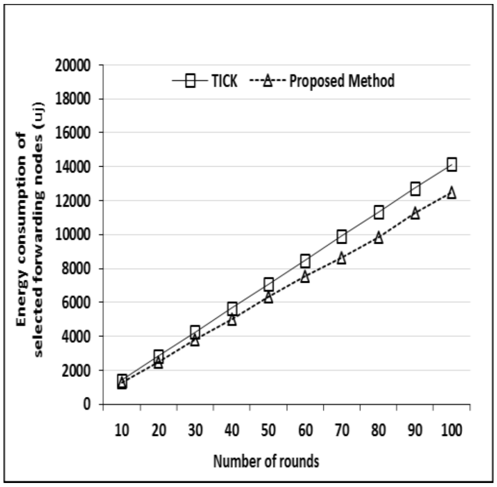

Figure. 5: Energy Consumption for Forwarding Nodes (µj) Versus Number of Rounds

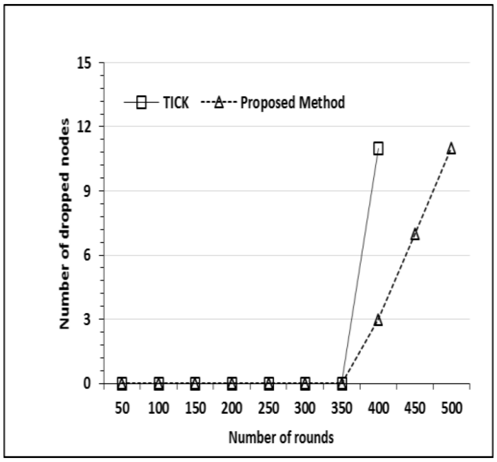

Figure. 4: Network Lifetime

5. Conclusion

Time-Based Dynamic Keying and En Route Filtering (TICK) provides network security and minimizes the communication cost. This is accomplished by eliminating control keying messages that cause depletion of a large amount of energy for each event sensing and forwarding node. Although this method is more energy-efficient and performs well in securing events as they occur, it allocates pre-decided selective nodes for re-encryption, which consumes more energy because it does not consider network parameters (such as the remaining energy of the filtering nodes, and the distance between two encrypting nodes). In order to address these issues, we proposed an energy-efficient method that helps select forwarding nodes for the re-encryption operation based on two network factors: the remaining energy of the forwarding nodes and the hop count. The proposed method improves energy conservation and extends the network lifetime. The simulation results validate the effectiveness and efficacy of the proposed method.

Acknowledgments

This research was supported by the Basic Science Research Program through the

National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484).

References

[1] P. Rawat, K. D. Singh, H. Chaouchi and J. M. Bonnin, “Wireless sensor networks: a survey on recent developments and potential synergies,” J Supercomput., Springer, vol 68, pp. 1-48, April 2014.

[2] M. Xie, S. Han, B. Tian and S. Parvin, “Anomaly detection in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol 34, pp. 1302-1325, July 2011.

[3] C. Karlof and D. Wanger, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, Elsevier, pp.293-315, 2003.

[4] A. S. Uluagac, R. A. Beyah and J. A. Copeland, “Time-Based Dynamic Keying and En-route filtering (TICK) for wireless sensor networks,” Proc. of IEEE GLOBECOM, pp. 1-6, December 2010.

[5] Z. Yu and Y. Guan, “A dynamic en-route scheme for filtering false data injection in wireless sensor networks,” Proc. of IEEE INFOCOM, pp. 1–12, April 2006.

[6] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” IEEE JSAC, vol. 23, no. 4, pp. 839–850, April 2005.

[7] R. Lu, H. Zhu, X. Liang and X. Shen, “BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol 31, no. 1, pp. 32-43, January 2012.

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” in Proc. of ACM MOBICOM, pp. 56–67, August 2002