International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 2, March-April 2019, pp. 175-188. Article ID: IJARET_10_02_018
Available online at http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

A KEY LEVEL SELECTION WITHIN HASH CHAINS FOR THE EFFICIENT ENERGY CONSUMPTION IN WSNS

Dr Syeda Gauhar Fatima
Professor ECE dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Syeda Kausar Fatima
Associate Professor, Shadan College of Engineering and Technology, Hyderabad, India

Dr Syed Abdul Sattar
Principal, Nawab Shah Alam Khan College of Engineering and Technology,
New Malakpet, Hyderabad, India

Naseer Ahmed Khan
Student, ECE Dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Syed Adil
Student, ECE Dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

ABTRACT

A wireless sensor network is comprised of a base station (BS) and numerous sensor nodes. The sensor nodes lack security because they function in an open environment, such as the military. In particular, a false statement injection attack seizures and compromises sensor nodes. The attack then causes the compromised nodes to create forward false reports. Due to the false report injection attack, not only does the sensor network have a false alarm, but its limited energy is also emptied. In order to preserve the false report injection attack, over the past few years, several studies have been made looking for a resolution to the attack. Ye et al. studied statistical en-route filtering (SEF). SEF is a method of randomly verifying event reports in the en-route filtering phase. SEF can filter many false reports early using proof of intermediate nodes. However, because the number of keys in a sensor node is fixed by the system, the sensor network cannot control the event report proof probability depending on the conditions of the network. Therefore, it is tough to proficiently consume energy of the sensor network. In order to resolve the problem, we suggest a technique which controls the event report verification probability by using a key sequence level of an event report. In

the suggested method, when an intermediate node obtains an event report, the node authenticates the event report by relating a key sequence level of the report and its key sequence level. Elements defining the key sequence level comprise the concentration of neighbor nodes in the sensing range of a center of stimulus (CoS), the number of stages from the CoS to the BS, and the average of the key sequence level of intermediate nodes in each track. We imitated the projected technique and the SEF technique to assess the performance in terms of energy efficiency and security. In the recreation results, the projected technique disbursed an average of 7.9% less energy of the sensor nodes compared to SEF method. The number of untrue reports inward at the BS of the proposed technique was also fewer, by an average of 6.4, compared to the SEF technique. Concluded the results, we can understand that when the number of false report is huge in the sensor network, the proposed technique is more energy-efficient and protected than the SEF technique.

Keywords: Wireless sensor network, False report injection attack, Statistical en-route filtering, Energy Efficiency, Security.

Cite this Article: Dr Syeda Gauhar Fatima, Syeda Kausar Fatima, Dr Syed Abdul Sattar, Naseer Ahmed Khan and Syed Adil, A Key Level Selection within Hash Chains for the Efficient Energy Consumption in WSNS, *International Journal of Advanced Research in Engineering and Technology*, 10(2), 2019, pp. 175-188.
http://iaeme.com/Home/issue/IJARET?Volume=10&Issue=2

1. INTRODUCTION

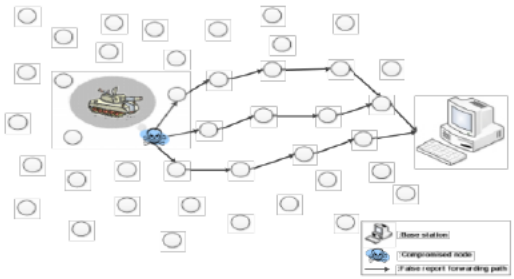


Fig. 1. The operation of a false report injection attack

Wireless sensor networks comprise of a huge amount of sensor nodes, which comprise sensing, computation, and wireless communication capabilities [1, 2]. The sensor nodes are assigned in a specific sensor field and operate each other collaboratively [1]. When an event arises in the sensor field, the nodes sense and calculate data of the event. The nodes also headfirst the data of the event to a BS [2]. The BS forward the data to a user through the prevailing communication infrastructure. Because the sensor networks function in exposed situations such as a military atmosphere, the scopes of the nodes are minor and unmanned [3, 4]. Therefore, the nodes are seized and conceded effortlessly by an invader from the external [2]. A false report injection attack particularly grounds a conceded node to create a false report. Fig. 1 shows the action of a false report injection attack. In Fig. 1, because of the false report generation of the conceded node in the sensor networks, the outbreaks lead to not only to false alarms, but also to the diminution of the limited energy of the sensor nodes, thus reducing the lifespan of the networks [4]. In order to protect the false report injection attack, a lot of resolutions have been projected by many scientists [4-14]. Ye et al. projected a resolution which is called SEF [4]. In SEF, each intermediate node confirms an event report using verification keys stochastically. The nodes headfirst the event report to the following node or drop it conditional on the verification outcomes. When the event report is untrue, the report is released. Thus, the false report is speckled initially by SEF. Though, the number of authentication keys comprised in a node has

to be big for advanced verification of false report possibility. If the numeral of keys of the node is additional, then the energy consumption of the node is higher. The quantity of keys is not attuned depending on the condition of the networks because it is static by the system. This means that it is problematic for the networks to be functioned proficiently. In order to resolve the problem, we projected a technique which regulates the confirmation chance of the node using a scheme of a key sequence level. The key sequence level is an index in a hash chain of a key, which types a message authentication code (MAC) in the event report. In the projected technique, the BS selects the key sequence level of an event report. Intermediate nodes getting the event report confirm it by equating the key sequence level of the node's key with the level of a MAC in the event report. The key sequence level is established by a fuzzy system in the BS. The fuzzy inputs defining the level are the regular of the level of nodes in each path furthering an event report, the compactness of neighbor nodes of a CoS, and the amount of hop from the CoS to the BS. The projected technique comprises security and competent energy consumption of sensor nodes by defining the suitable key sequence level. The rest of this paper is ordered as follows. Section 2 defines the SEF. Section 3 describes the problem statements. Section 4 presents a system model of the projected technique and the operation process of the proposed method. Section 5 shows the simulation results to estimate the performance of the projected technique. Finally section 6 accomplishes this paper.

2. BACKGROUND

2.1. Statistical en-route filtering

SEF is a countermine technique which can filter false reports early on that are made by a compromised node in a wireless sensor network using statistical verification during the en-route filtering phase. SEF consists of three phases: key assignment and report generation, en-route filtering, and sink verification. In the key assignment phase, before the sensor nodes are organized in a sensor field, each node obtains some keys where the amount is fixed by the system casually from a particular partition at random in the global key pool. In the report generation phase, after the nodes are organized, sensing nodes detecting the event elect a CoS when an event occurs in the sensor network. They frontward a partition index and a MAC to the BS which was created by a key that each node comprises to a BS. The CoS creates an event report with the event information and the received MACs and forward the event report to the BS. In the en-route filtering phase, when an intermediate node obtains the event report, it approves the report stochastically. The node checks whether there are key indices of distinct partitions and MACs in the report. If there is also more than one key index or less than the one in the same partition or the amount of them in the report does not resemble with the amount of fixed MACs, the node favors the report as a false report and drops it. The node then inspects whether there is a key index in the report consistent with the key index of the node. If there is not a key index, the node forward the report to the next node. If not, the node generates a MAC using its key. It then equates the MAC with the MAC in the report. If the MAC of the node is dissimilar from the MAC in the report, the report is viewed as a untrue report and is dropped. Else, the report is observed as a valid report and is promoted to the next node. In the sink verification phase, all of the event reports received at the sink are substantiated, because the sink comprises all keys in the global key pool. Thus, it can filter untrue reports out the false reports that are not filtered in the enroute filtering phase.

3. PROBLEM STATEMENT

If a false report injection attack arises in a wireless sensor network, a compromised node will unceasingly produce numerous false reports, furthering them to a BS. When the amount of compromised nodes becomes higher, the amount of untrue reports becomes greater. The sensor

network which connects many false reports may easily breakdown because of the energy reduction of the sensor nodes in the network. In SEF, a illustrative countermine technique, in order to preserve the network against the attack, intermediate nodes authenticate event reports using their allocated key before they are arranged in a sensor field. The key number is a very vital element defining the verification possibility of the report. The number of key that a node comprises becomes bigger, the possibility becomes higher. However, the node has to consume a lot of verification energy. Also, when an attacker compromises a node, the number of keys that the attacker can get becomes greater. On the other hand, as the number of keys becomes lesser, the probability becomes smaller. However, the energy consumption used in the verification becomes lower. Subsequently, the number of keys that the attacker can get becomes smaller. Therefore, in order to proficiently operate the sensor network, it is vital to trade energy consumption for security. Increasing the number of keys that the node includes is difficult in SEF because the energy of the sensor nodes is limited. To solve the problem, we use a key sequence level scheme. The scheme helps decrease the energy consumption and make up for security. Section 4 describes the proposed method using the key sequence level.

4. PROPOSED METHOD

4.1. System model and assumption

A wireless sensor network contains of a BS and numerous sensor nodes. The BS contains a global key pool. In the global key pool, there are all the keys which are used in the sensor network. The BS also includes a fuzzy system that calculates a key sequence level. The BS knows the average of the key sequence level of the intermediate nodes which forward event reports in each path, the density of neighbour nodes of the CoS, and the number of stages from the CoS to the BS. The concentration of sensor nodes in the network is very high, and each node is small and each node contains simple computing capability and limited energy.

4.2. Operation

4.2.1. Key assignment and report generation

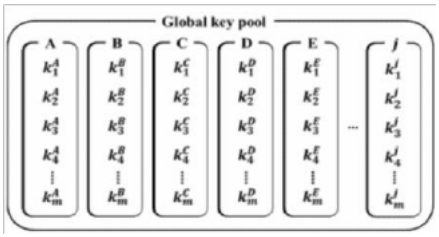


Figure 2 A global key pool which consists of j hash chains

In Figure 2, a hash chain is made up of m keys. The last sequence key in each hash chain k_m^j is a seed key of each hash chain. The next sequence key is consequent using a hash function with the seed key.

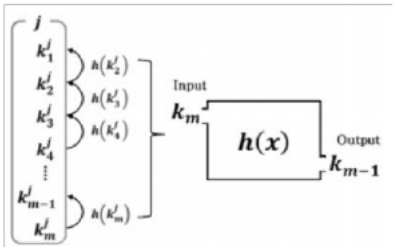
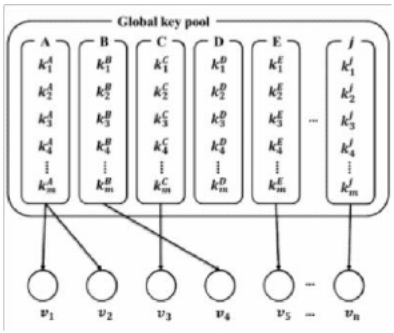


Figure 3 Derivation of keys using the hash function

In Figure 3, if the hash function receives a seed key as an input, the hash function outputs the derived key k_{m1}. If the hash function receives k_{m1} as an input, then it outputs a derived key k_{m2}. This process is repeated until the function outputs the key k_1. The derived keys are allotted to sensor nodes before the sensor nodes are organized in the sensor network.



$v_1 \text{key} = k_{46}^{A}$

$v_2 \text{key} = k_{4}^{A}$

$v_3 \text{key} = k_{19}^{C}$

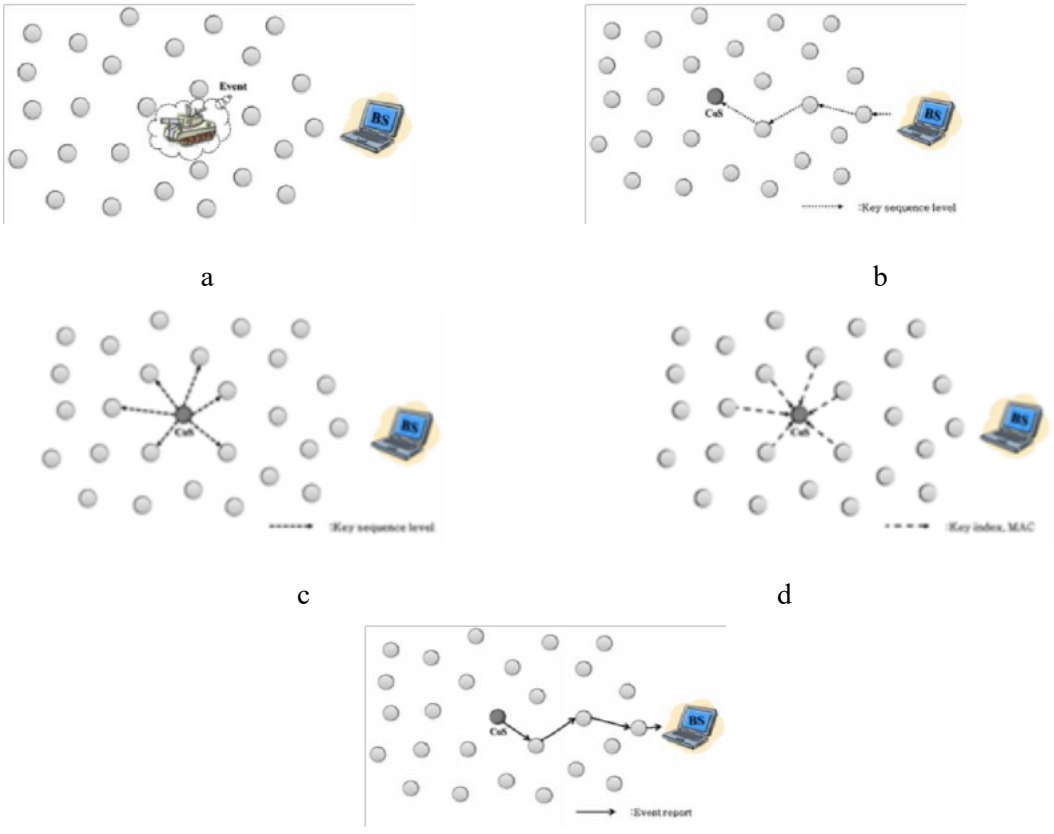
$v_4 \text{key} = k_{27}^{B}$

$v_5 \text{key} = k_{38}^{E}$

(a) (b)

Figure 4 Example of an operation of key assignment in a global key pool (Fraction of m = 50)

Figure 4 (a) shows that just one key is casually allotted to each sensor node $v_1 \sim v_n$. Figure 4 describes an example of the keys which are assigned to the sensor nodes. The sensor nodes originate other keys from the allocated key and a hash table. For example, In Fig. 4, a node v_3 receives a key k_{19}^{C} in the C hash chain of the global key pool and then v_3 can get the keys from k_{18}^{C} to k_1^{C} using the hash function.



a b

c d

e

Figure 5 The operation of a report generation

When an event arises in the sensor field, numerous sensing nodes distinguish the event, as seen in Fig. 5 (a). The sensing nodes elect a CoS, which is a node that strongly notices the event. After the election of the CoS, the BS forward the key sequence level, which is determined by a fuzzy system, to the CoS, as seen in Fig. 5 (b). The CoS forward the key sequence level to its neighbor nodes in Fig. 5 (c). The neighbor nodes then create MACs using the equivalent keys with material of the key sequence level from the CoS forwarding the MACs. A node which does not include the corresponding key with the key sequence level does not forward the MAC to the CoS, as seen in Fig. 5 (d). The CoS creates an event report using its information of the event and acknowledged MACs from the neighbor nodes. It then forwards the event report to the following node in Fig. 5 (e, f).

4.2.2. The scheme of key sequence level

The key sequence level is a generation index of a key, which makes a MAC in the event report in a hash chain. The key sequence levels of MACs in the event report are the same.

4.2.2.1. Elements determining a key sequence level

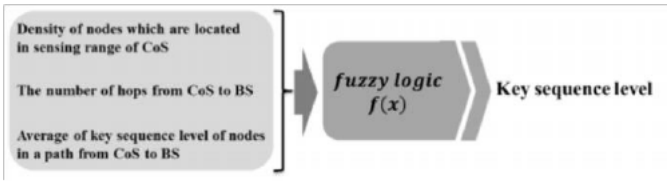


Figure 6 Elements determining a key sequence level

In Fig. 6, the fuzzy system calculates three input values in order to get the key sequence level as an output value. The three input values are the concentration of neighbor nodes, which are situated within the sensing range of a CoS, the amount of hops from the CoS to a BS, and the average of the key sequence levels of intermediate nodes in a path.

4.2.2.1.1. Density of neighbour nodes which are located in sensing range of a CoS

The higher the concentration of neighbor nodes in the CoS, the more the CoS collects MACs equivalent with the key sequence level. For instance, let's suppose the key sequence level is 6 and the number of neighbor nodes in the sensing range of the CoS is 20 or 30. In the case of 30, the CoS gathers more MACs corresponding to key sequence level 6 than in the case of 20. If the possibility of the collection of MACs is higher, although the key sequence level is high, the CoS will assemble enough MACs corresponding to the fixed number of MACs in the event report. Thus, the higher the density, the higher the key sequence level. On the other hand, the lower the concentration is, the lower the key sequence level is.

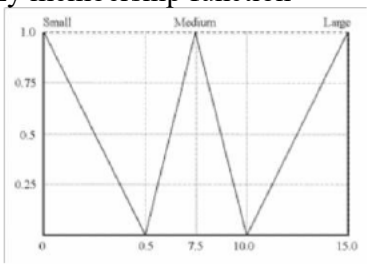
4.2.2.1.2. The number of hops from a CoS to a BS

In order to reduce the energy consumption of the sensor nodes, false reports have to be eliminated early. The more hops there are from the CoS to the BS, the more sensor nodes forward the event report, and a great amount of energy of the sensor nodes is consumed. Therefore, when the number of hops is big, the key sequence level has to be lower, and the report verification probability has to be high. On the contrary, when the number of hops is minor, the key sequence level has to be high and the probability has to be lower.

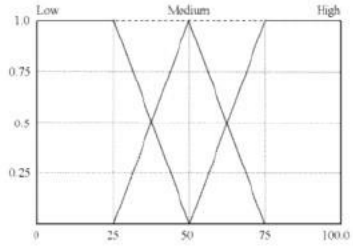
4.2.2.1.3. The average number of key sequence levels of intermediate nodes in a path

The average number of key sequence levels of the forwarding node in each path is a very significant element defining the key sequence level of the event report, because when the average of the key sequence level is high, the report verification possibility becomes high, and when the average is lower, the probability becomes lower. Thus, the higher the average is, the

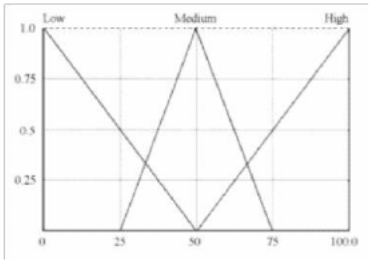
higher the probability is. On the other hand, the lower the average is, the lower the probability is. Fuzzy membership function



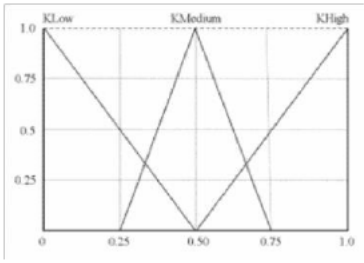
(a) The number of hops from the CoS to the BS



(b) Density of neighbor nodes in a sensing range of the CoS



(c) The average of the key sequence level of intermediate nodes in each path



(d) Key sequence level of an event report

Figure 7 Membership functions of input and output elements

In Fig. 7, (a) is a membership function of the number of hops from a CoS to the BS, (b) is the membership function of the concentration of neighbor nodes in the sensing range of the CoS, and (c) is a membership function of the average of the key sequence level of intermediate nodes in each path. In the membership function (a), fuzzy values are comprised in the fuzzy set which contains of three levels. The three levels are Low, Medium, and Large. In the membership functions (b) and (c), the fuzzy values are comprised in the fuzzy set. The fuzzy set contains of Low, Medium, and High. The membership function (d) is a membership function of a key sequence level of an event report. Its fuzzy values are comprised in a fuzzy set. The fuzzy set is composed of KLow, KMedium, and KHigh. In all fuzzy membership functions, the fuzzy values are in the range from 0-1.

4.2.2.2. Fuzzy rules

Table 1 Fuzzy rules of the proposed method

No.		**INPUT**		**OUTPUT**
0	NUM_HOP	NEIGHBOR_DENSITY	AVERAGE_KEYLEVEL	KEY_LEVEL
	Small	High	High	KHigh
4	Small	Medium	Medium	KHigh
8	Small	Low	Low	KHigh
9	Medium	High	High	KMedium
12	Medium	Medium	High	KMedium
15	Medium	Low	High	KMedium
20	Large	High	Low	KLow
22	Large	Medium	Medium	KLow
26	Large	Low	Low	KLow

In Table1, NUM_HOP, NEIGHBORRR_DENSITY, and AVERAGE_KEYLEVEL are fuzzy inputs. NUM_HOP is the amount of hops that an event report has to pass from a CoS to a BS. NEIGHBOR_DENSITY is concentration of neighbor nodes in a sensing range of the CoS. AVERAGE_KEYLEVEL is the average of the key sequence levels for the sensor nodes in each path. KEY_LEVEL is a fuzzy output and the key sequence level of the event report.

4.2.3. En-route filtering

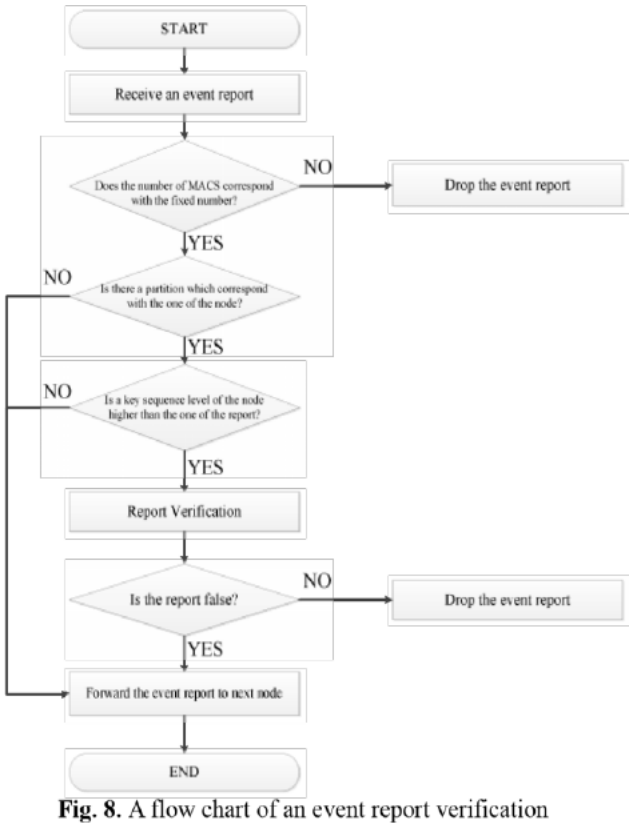


Fig. 8. A flow chart of an event report verification

Once the node obtains the event report, it checks whether the number of MACs in the event report matches with the fixed number of MACs in the system (a). If the two number are dissimilar, the node regards the event report as a false report and drops the it (b). Otherwise, the node inspects whether there is a corresponding partition in the event report with its partition of MACs (c). If there is not a partition, it forwards the event report to the next node (d). If there is a corresponding partition, the node equates the key sequence level of its key with the key sequence level of the MACs in the equivalent partition (e). When the key sequence level is lower than the one in the event report, it forwards the report to the next node (f). Instead, when the key sequence level is the same or higher than the one in the event report, it creates a MAC using its key and equates the MAC with the MAC of the event report (g, f). If the two MACs are the same, it regards the event report as a authentic node and forwards the report to the next node (i). Else, it regards the report as a false report and drops it (j).

4.2.4. Base station verification

When event reports arrive at a BS, the BS will verify all the MACs in the event reports because it includes a global key pool. If the BS receives an event report, it finds a key that matches to the key sequence level of a MAC in the event report. If there is a key, the BS generates a MAC using the key. It then compares the MAC with the MAC in the event report. If the two MACs are not the same, the BS drops the event report. Thus, although there are false reports which are not filtered in the en-route filtering phase, the BS verifies all false reports during this phase.

5. SIMULATION

In section 5, we equate the energy efficiency and security of our projected technique with that of the SEF in order to evaluate the performance of the proposed method. We evaluate the energy consumption of the sensor nodes versus the rate of false reports based on the number of compromised nodes among the sensing nodes, which generate MACs included in an event report, so as to equate the energy efficiency of the proposed method to that of the SEF. The number of false reports means arrivals at the BS which are not filtered in the en-route filtering phase. We also equated the number of false reports versus the rate of false reports in the proposed method to that of the SEF, so as to estimate security.

Section 5.1 describes our simulation environment. Section 5.2 presents the simulation results.

5.1. Simulation environment

Table 2 A simulation environment

Content	Values
The number of the whole sensor nodes in a sensor network	600
The area of a sensor field	100m X 100m
A sensing range of a sensor node	10.0m
Energy consumption per 1byte when a sensor node sends an event report	16.25 μJ
Energy consumption per 1byte when a sensor node receives an event report	12.5 μJ
Energy consumption of an event report verification of a sensor node	75 μJ
The number of hash chains in a global key pool	10
The number of MACs in an event report	5
The number of occurring event reports in a sensor network	100
The number of keys in a hash chain	50
The number of keys included in a sensor node.	25
The packet size of an event report	24bytes

5.2. Simulation results

In the simulation results, the rate of false reports is the entire number of event reports in the sensor field versus the number of false reports. The energy consumption is the sum total of the energy consumption of all of the sensor nodes in the sensor field.

Fig. 9 is a graph of energy consumption versus the rate of false reports in the projected technique and the SEF method when a sensing node which creates a MAC included in the event report is conceded.

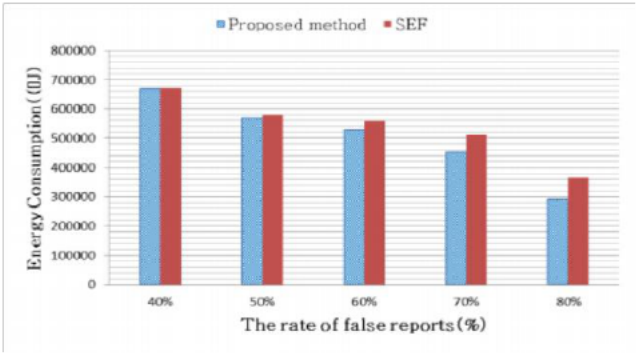


Figure 9 Energy consumption versus the rate of false reports (Fraction of compromised node = 1)

In Fig. 9, we found that the projected technique consumes less energy of the sensor nodes than the SEF method. We also found that the higher the rate of false reports, the larger the gap between the energy consumption of the proposed method and SEF method. In the simulation result, the proposed method consumed an average of 7.89% less energy than the SEF.

Fig. 10 is a graph of the number of false reports arriving at the BS in the proposed method and the SEF method when a sensing node which creates a MAC included in the event report is compromised.

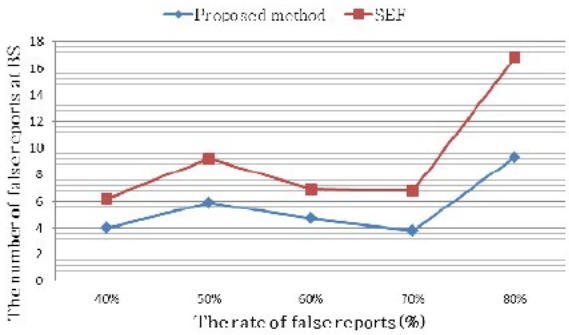


Figure 10 The number of false reports versus the rate of false reports (Fraction of compromised node = 1)

In Fig. 10, we found that the amount false reports arriving at the BS in the proposed method is less than in the SEF method. In the simulation result, the number of false reports of the projected technique is an average of 3.64 less than in the SEF method.

Fig. 11 is a graph of energy consumption versus the rate of false reports in the projected technique and in the SEF method when the two sensing nodes which create MACs included in the event report are compromised.

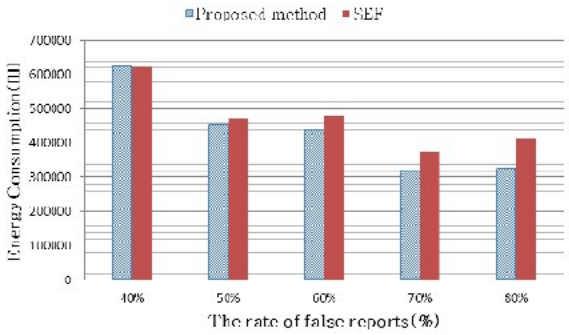


Figure 11 Energy consumption versus the rate of false reports (Fraction of compromised nodes = 2)

In Fig. 11, the higher the rate of false reports is, the larger the gap between the energy consumption of the projected technique and that of the SEF method. We also know that the proposed method consumes less energy than the SEF. In the simulation result, the proposed method consumed an average of 9.09% less energy than the SEF.

Fig. 12 is a graph of the number of false reports arriving at the BS in the projected technique and that of the SEF method when two sensing node which generate MACs included in the event report are compromised.

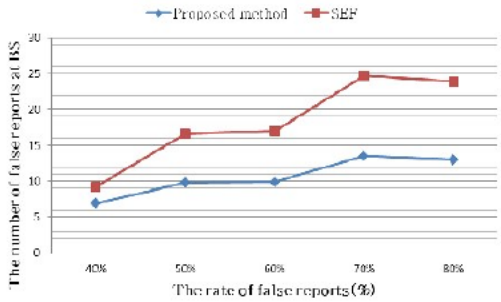


Figure 12 The number of false reports versus the rate of false reports (Fraction of compromised nodes = 2)

In Fig. 12, we found that the amount of false reports arriving at the BS in the projected technique is less than that of the SEF method when the two nodes are compromised. In the simulation results, the number of false reports is 7.66 less than that of the SEF method.

Fig. 13 is a graph of the energy consumption versus the rate of false reports in the proposed method and that of the SEF method when three sensing nodes which generate MACs included in the three event reports are compromised.

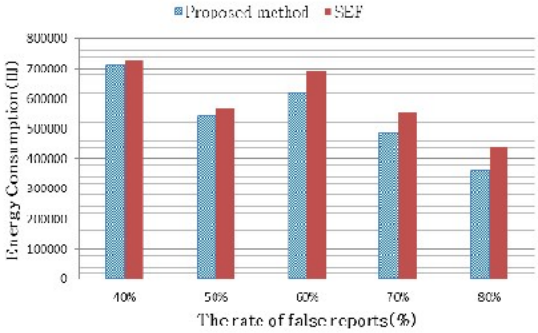


Figure 13 Energy consumption versus the rate of false reports (Fraction of compromised nodes = 3)

In Fig. 13, the projected technique spent less energy than the SEF. The higher the rate of false reports, the larger the gap of energy consumption is between the projected technique and the SEF method. In the simulation result, the proposed method consumed an average of 9.26% less energy than the SEF.

Fig. 14 is a graph of the number of false reports incoming at the BS in the proposed method and that of the SEF method when three nodes which create MACs included in an event report are compromised.

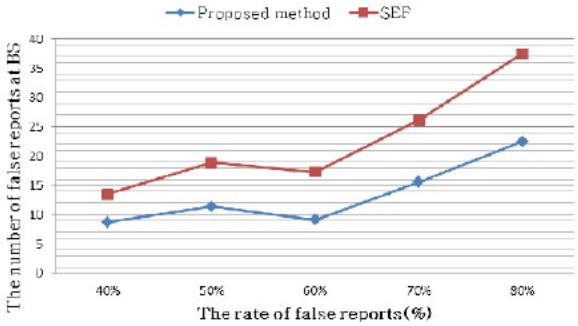


Figure 14 The number of false reports versus the rate of false reports (Fraction of compromised nodes = 3)

In Fig. 14, we found that the number of false report incoming at the BS in the projected technique is less than that of the SEF method. In the simulation result, the number of false reports was 9.22 less than in the SEF.

Fig. 15 is a graph of the energy consumption versus the rate of false reports in the proposed technique and in the SEF when four sensing nodes which create MACs included in the three event reports are compromised.

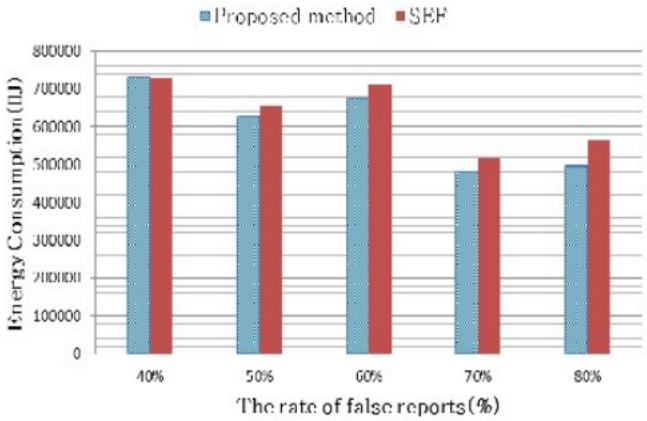


Figure 15 Energy consumption versus the rate of false reports (Fraction of compromised nodes =4)

In Fig. 15, when the rate of false reports is above 50%, the proposed method had better energy efficiency than the SEF. In the simulation result, the proposed method consumed an average 5.63% less energy than the SEF.

Fig. 16 is a graph of the number of false reports arriving at the BS in the proposed method and in the SEF when four nodes which create MACs included in the event report are compromised.

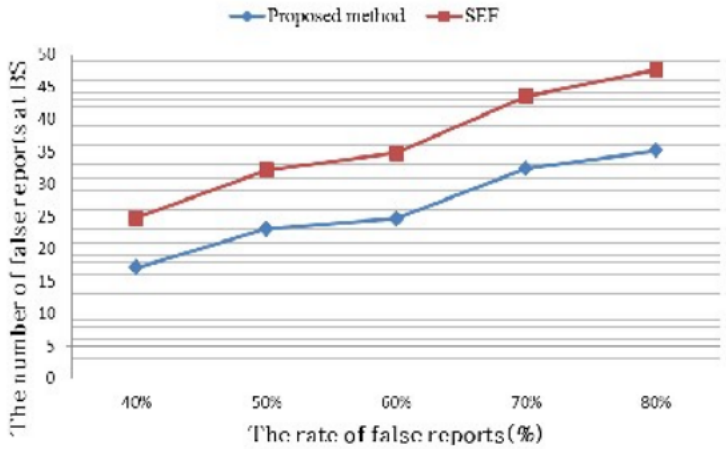


Figure 16 The number of false reports versus the rate of false reports (Fraction of compromised nodes = 4)

In Fig. 16, we found that the number of false report incoming at the BS in the proposed method is less than in the SEF for all of the false reports rates. In the simulation result, the number of false reports was 10.14 less than that of the SEF method.

In the simulation results, the proposed method was an average of 7.9% better than the SEF with respect to energy efficiency. The amount of false reports arriving at the BS in the proposed method was an average of 6.43 less than in the SEF method. We tested that the higher the rate

of false reports in the sensor network, the better energy efficiency and security there was in the proposed method compared to the SEF method.

6. CONCLUSION

In this paper, we proposed a resolution which regulates the key sequence level of MACs included in an event report and verifies them by comparing the key sequence level of the MACs in the event report with the key sequence level of a node which receives the event report. This is done in order to preserve energy efficiency so when the possibility of a false report in the event report is high, the event report verification probability is low, and the energy consumption of the sensor nodes is low. On the other hand, when the key sequence level is low, the event report verification probability is high, and energy consumption is high. Thus, it is important to determine an appropriate key sequence level. In order to determine the appropriate key sequence level, it is computed by a fuzzy system in a BS. Elements determining the key sequence level are the density of neighbor nodes in a sensing range of the CoS, the number of hops from the CoS to the BS, and an average of the key sequence level of intermediate nodes in each path.

We estimated the energy efficiency and security of the proposed method by equating it to the SEF method, which is a representative countermeasure method against the false report injection attack. We measured the energy consumption of the sensor nodes versus the rate of false reports in the sensor network to evaluate the energy efficiency of either the proposed method or the SEF. Additionally, we also measured the number of false report received in the BS versus the rate of false reports to evaluate the security of either the proposed method or the SEF. In the simulation results, the proposed method consumed an average of 7.9% less energy of the sensor network. Moreover the number of false reports arriving at the BS in the proposed method was an average 6.4 less than in the SEF method. It was found from the result that the projected technique has better energy efficiency and security than the SEF when the rate of false reports is high.

ACKNOWLEDGEMENTS

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

Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2013R1A2A2A01013971)

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci: Wireless sensor networks: a survey, Computer Networks, 38(4), 15 (2002) 393-422.

[2] Al-Karaki N., Kamal and A.E.: Routing techniques in wireless sensor networks: a survey, Wireless Communications, IEEE , 11(6), (2004) 6-28.

[3] Chris Karlof, David Wagner: Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks, 1, (2–3), (2003) 293-315.

[4] Fan Ye, Luo, H., Songwu Lu and Lixia Zhang: Statistical en-route filtering of injected false data in sensor networks, Selected Areas in Communications, IEEE Journal on , 23(4), (2005) 839- 850.

[5] Zhen Yu, Yong Guan: A dynamic en-route filtering scheme for data reporting in wireless sensor networks, IEEE/ACM, 18(1), (2010) 150-163.

[6] J. Hao Yang, Songwu Lu: Commutative cipher based en-route filtering in wireless sensor networks, Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th , vol. 2, (2004) 1223- 1227.

[7] Sencun Zhu, Setia, S., Jajodia, S. and Peng Ning: An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on , vol., no., (2004) 9-12, 259- 271.

[8] H.Y. Lee, T.H. Cho: Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks, Lect. Notes Comput. Sc, vol. 4371, Springer, Heidelberg (2006) 116–127.

[9] Zhang, W., Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach, In: Proc. of INFORCOM, (2005) 503– 514.

[10] Perrig, A., Szewczyk, R. and Tygar, J.D., Wen, V., Culler, D.E.: SPINS: Security Protocols for Sensor Networks. Wirel. Netw. 8(5), (2002) 512–534.

[11] B.H. Kim, T.H. Cho: Condition-based Key Dissemination Period Determining Method in Sensor Networks, In Proc. Of ICACT, (2008).

[12] S.J. Lee, H.Y. Lee and T.H. Cho: A Threshold Determining Method for the Dynamic Filtering in Wireless Sensor Networks Based on Fuzzy Logic, International Journal of Computer Science and Network Security, 8(4), Apr. (2008).

[13] M.H Han, H. Y. Lee and T.H. Cho: Fuzzy-Based Verification-Probability Determination Method for Dynamic Filtering in Sensor Networks, International Journal of computer Science and Network Security, 8(8), Aug. (2008) 132-136.

[14] H.Y. Lee, T.H. Cho: Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks, IEICE Transactions on Communications, E90-B(12), Dec. (2007) 3346-3353.

[15] Shashank Bholane and Devendrasingh Thakore, Sender to Receiver Synchronization in Wireless Sensor Networks – A Simulation Study, International Journal of Computer Engineering and Technology (IJCET), Volume 3, Issue 2, July- September (2012), pp. 265-270

[16] Poonam Thakur and M. Vijaya Raju, Survey on Routing Techniques For Manets and Wireless Sensor Networks: A Comparison, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, January- February (2013), pp. 275-283

[17] Anitha Christy P Angelin, Deva Priya Isravel and Diana Arulkumar Throughput Intensification for IOT Based Subversive Drainage Monitoring Applications In Wireless Sensor Networks, International Journal of Civil Engineering and Technology (IJCIET), Volume 9, Issue 11, November 2018, pp. 2186–2196

[18] Pardeep Kumar and Tanisha Saini, To Propose a Technique for Fault Tolerance in Wireless Sensor Networks. International Journal of Computer Engineering and Technology, 7(5), 2016, pp. 01–08

[19] Geetha.M, J.Prassanna, M.Nivedita and Prabhakaran.R, Towards an Enhanced Efficient Cross Layer Protocol (Eeclap) for Wireless Sensor Networks, International Journal of Mechanical Engineering and Technology 8(11), 2017, pp. 394–402.

[20] M.S. Doibale and Dr. G. D. Kurundkar, Wireless Sensor Networks Congestion and Role of Artificial Intelligence, International Journal of Computer Engineering and Technology, 10(2), 2019, pp. 60-66.

[21] Neeraj Tiwari, Rahul Anshumali and Prabal Pratap Singh, Wireless Sensor Networks: Limitation, Layerwise Security Threats, Intruder Detection, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 2, July- September (2012), pp. 22-31.