http://dx.doi.org/10.36785/jaes.111417

Improving TICK efficiency by GA-based fuzzy membership functions optimization in Wireless Sensor Networks

Tae Ho Cho [a], Muhammad Ashraf [b,*], Muhammad Akram [c], Hamayoun Shahwani [d], Syed Attique Shah [e], Surat Khan [d], Faizullah Khan [d], Akbar Khan [b] and Muhammad Qasim Khan [f]

[a] College of Computing, Sungkyunkwan University, Suwon, South Korea
[b] Department of Computer Engineering, BUITEMS, Quetta
[c] Department of Software Engineering,
[d] Department of Telecommunication Engineering,
[e] Department of IT, Department of computer Science, BUITEMS, Pakistan
[f] Faculty of Information and Communication Technology, BUITEMS, Quetta
[*]Corresponding author: muhammad.ashraf@buitms.edu.pk

***Abstract*-- In wireless sensor networks (WSNs), the energy and computational capacity of the sensor nodes are limited and they are deployed in a hostile environment. An adversary can easily compromise a sensor node and injects false data into the network. This injection of false data drastically depletes the energy of the nodes designated on the route for forwarding the source data. Many filtering methods have been proposed to tackle the security issues but they also increase the communication cost by exchanging the control keying messages which consumes more energy with in the network. Fuzzy logic for TICK was proposed to reduce the communication cost and increase the energy efficiency of the en-route nodes by selecting the re-encrypting nodes efficiently and avoiding the exchange of control keying messages in the network. Membership functions in the fuzzy system need to be optimized in order to use the fuzzy inferencing more efficiently. We propose an optimized fuzzy membership functions method by using genetic algorithm. The genetic algorithm determines the optimal membership functions which help in selecting the most favourite re-encrypting nodes in TICK based wireless sensor network. Simulation results show that the proposed method optimizes the membership functions and achieves better energy conservation at sensor nodes.**

***Keywords*- wireless sensor networks, en-route filtering, false report injection attack, energy efficiency, fuzzy logic, genetic algorithm.**

Date Received: 14-10-2020
Date Accepted: 26-10-2020
Date Published: 08-06-2021

I. INTRODUCTION

Latest technological research advancement has ensured the deployment of low-cost, limited computational and low powered distributed devices. These devices are known as sensor nodes and a collection of such nodes is called sensor network. Each node in the network has the capability to observe a given physical environment despite of its low storage, stringent energy resources and limited data processing capabilities. A group of such sensor nodes can coordinate with each other and perform specific functions. These nodes are used in different applications such as health care, smart buildings, animal tracking, agricultural and environmental monitoring [1,2]. As sensor nodes are deployed in a hostile environment and left unattended without any infrastructure, an adversary can easily compromise some nodes in the network and launch different types of attacks such as insider attacks, outsider attacks, passive attacks, active attacks and attacks over the layers of network devices [3]. Furthermore, sensor nodes have limited and irreplaceable energy resources [4]. Therefore, it is more important to provide security against these attacks and ensure energy efficiency in the network. As a solution several energy efficient, en-route filtering, key management, data aggregation, and authentication schemes have been designed.

Several data filtering schemes [5-8] have been proposed to detect and filter false data injected into the network. Although these schemes provide strong resilience against some attacks and filter malicious data, but most of them are lacking in providing the energy efficiency by exchanging control keying and re-keying messages to refresh keys in the network [9] and causing high communication costs associated. Time-based Dynamic Keying and En-Route Filtering (TICK) [10] and Secure SOurce-BAsed Loose Synchronization (SOBAS) [11] were proposed to address these issues and minimize the communication cost. TICK achieves high energy savings by eliminating the exchange of control messages regarding keying or rekeying and further utilizes a small portion of these energy savings in the computation of local security services. SOBAS [11] exploits the TICK framework and provides re-encryption

for forwarded reports at multiple preselected intermediate nodes that are at equal distances from one another.

Energy Efficiency Enhancement of TICK –based Fuzzy Logic (EETF) in WSNs [12] was proposed to overcome the flaws observed in TICK and SOBAS by selecting most favourite forwarding nodes for re-encryption operation and improved the energy efficiency of en-route nodes in the network. But membership functions are not optimized and need to be optimize to perform well and to further improve the energy efficiency of the network. We propose membership function optimization of [12] by using genetic algorithm. Our proposed method determines the fittest values for the membership functions which helps in selecting the favourite forwarding nodes for re-encryption operation.

IS document is an example of the desired layout for a JAES Journal paper. It contains information regarding desktop publishing format, type sizes, and typefaces. Style rules are provided that explain how to handle equations, units, figures, tables, a bbreviations, and acronyms. Sections are also devoted to the preparation of acknowledgments, references, and authors' biographies.

II. Related Work

To detect and filter malicious data from the WSN, several en-route data filtering methods have been proposed. Some of them are; Statistical En-route Filtering (SEF) [5], Dynamic En-route Filtering (DEF) [6], An Interleaved Hop-by-Hop Authentication (IHA) [7] and Commutative Cyber based En-route Filtering (CCEF) [8]. In [5], to validate each report, SEF uses different message authentication codes (MACs) which increases the size of each report due to MAC overhead. This effects the energy consumption of each report travelling from the source to Base Station (BS). In [6], significant amount of energy is used to verify the coming reports because DEF employs separate authentication keys in several nodes to endorse legitimate reports. In [7], IHA filters the malicious data in the presence of compromised nodes less than a threshold (t nodes). If compromised nodes are more than t nodes then it cannot filter the malicious data which limits the filtering capacity. In [8], CCEF filters the malicious data by using a session key which is encrypted, and un-encrypted witness key in the Query message. CCEF is based on a public key algorithms which needs more energy for the commutative ciphering. Although these schemes provide strong resilience against the false injected report attack but these are not necessarily energy efficient as they exchange control messages for keying and thus increase the communication cost of the network.

To minimize the communication cost, Time-based Dynamic Keying and En-Route Filtering (TICK)[10] and Secure SOurce-BAsed Loose Synchronization (SOBAS) [11] were developed. In [10], the incoming report is encrypted with one time dynamic key generated by the node using its own local time value and the verification node validates the report by decoding the report using the key generated by its own local time value. Thus TICK sends reports to the base station without exchanging the control keying messages and minimizes the communication cost of the network. SOBAS in [11] uses the frame work of [10] and employs the encrypting strategy to reduce the false positive rate (PFR) experienced in TICK and further improves the energy efficiency of the network.

In [12], we presented a fuzzy logic based source authentication technique which helps to very data reports at the intermediate nodes. Our proposed scheme enables the adaptive selection of a number of such verification nodes aimed at saving computational energy at low false positive report rate and increased security at higher false positive report insertion rate. In [13], authors proposed the adaptive forwarding node selection method using fuzzy logic. This method uses the PVFS framework and selects most favourite nodes for data verification. In [14], a reliable data delivery path based on fuzzy logic is presented. The proposed method selects reliable path considering the network parameters such as the energy status of the nodes in the network and the number of the false reports generated in the network.

III. Background and Motivation

A. Background

Our proposed method [12] employs fuzzy rule based system to select most favourite en-route nodes for re-encryption operation in TICK-based sensor network [10]. The method considers the network parameters such as

- Remaining energy level (ERL) of the en-route nodes
- Hop count (HC) between two encrypting nodes
- False positive rate (FPR)

These network parameters makes sure the adaptive selection of a number of such verification nodes aimed at saving computational energy at low false positive report rate and increased security at higher false positive report insertion rate.

B. Motivation

Knowing that fuzzy rule-based system is a best option to be used in the presence of imprecision in data and uncertainty in reasoning and inferencing process. In [12] membership functions are carefully selected through simulation to get desirable results. To make the best use of fuzzy rule-based system, their membership functions need to be optimized. The optimized membership function further improves the performance of the fuzzy system. Manual optimization of fuzzy membership function is unfeasible because it takes much human expertise and time. So genetic algorithm (GA) becomes the best option to optimize the membership function of [12]. We propose an efficient method based on genetic algorithm which assesses the fitness of membership functions through simulation outcomes and optimizes them through GA based evolution process.

IV. PROPOSED METHOD

A. Overview

Our proposed method utilizes the basic functional framework of [12] and modifies the membership functions of the fuzzy rule based system used in [12]. To further improve the performance of fuzzy system, membership functions are equally important to be optimized. For the optimization of fuzzy membership functions, we take the advantages of using genetic algorithm. We aim to select more suitable en-route nodes for re-encryption operations with the help of using optimized membership functions which can save further energy by dropping the malicious data early and passing the true data and minimizes the false positive rate in the network.

B. System Model and Assumptions

We assumed a wireless sensor network having sensor nodes and a base station (BS) where sensor nodes are densely deployed. Sensor nodes are low powered, less computational capability and short range devices. Sensor nodes remain static after they are deployed and have same range of communication and same initial energy. We also assumed that all nodes are assigned a network initialization vector (IV) and they are synchronized at pre-deployment phase. On other side BS is considered to have high storage capacity, computation power and unlimited energy resources. In addition, we assumed that only outsider can inject false reports so insider attacks are not considered in our work.

C. GA-based Membership Functions Optimization

Genetic algorithm is a heuristic search method based on natural evolution and is more reliable in solving optimization problems [15, 16]. GA has been used in many optimization applications such as function optimization and neural network optimization etc. [17]. In GA [18], a population pool is initiated by random functions or selected from the previous near optimal solutions which is consisted of different individuals. Each individual is generally known as chromosome (possible solution) and is represented by a finite sequence of zeros and ones. Each member (i.e., 0 or 1) of a chromosome is called gene. Some chromosomes are then selected based on their fitness values from the population as parents and undergoes through operations and generates new offsprings. The new generated offsprings then replace the chromosomes having least fitness value in the population. This process repeats until a termination condition reaches or optimal solutions achieves. The different steps used in a GA operation are illustrated in fig. 1.

In our proposed scheme, the first step is to initialize the population. A single chromosome is used to represent a set of the input parameter of the membership function in one trail. The input parameters are remaining energy level (REL), hop count (HC) and false positive rate (FPR) whereas the labels of each input parameter are small (SM), Medium (MD) and large (LG) for remaining energy level, near (NR), middle (MD) and far (FR) for hop count and very low (VL), low (LW), medium (MD), high (HG) and very high (VH) [12].

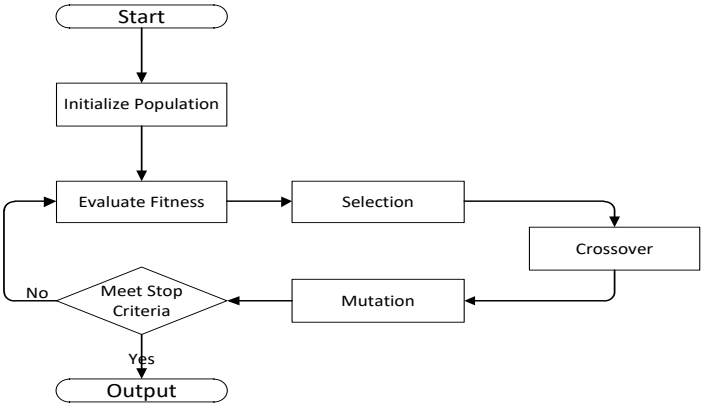


Fig. 1. GA flow chart

As the fuzzy system uses 3 triangular membership functions of REL and HC and 5 triangular membership functions of FPR thus the fuzzy system makes 45 (3*3*5) fuzzy rules. The input parameters and their chromosomes in our proposed scheme are shown in the fig. 2.

Each parameter of REL, HC and FPR are coded by 7 digits and thus each chromosome is comprised of (7+7+7) = 21 bits for REL, (7+7+7)=21bits for HC, and (7+7+7+7+7)= 35bits for FPR. In our proposed scheme, 200 generations are created where each generation comprising of 20 chromosomes, therefore 4000 trials are carried out for the network parameters REL and HC whereas 300 generations are created where each generation comprising of 30 chromosomes, therefore 9000 trials are carried out for the network parameters FPR in the simulations.

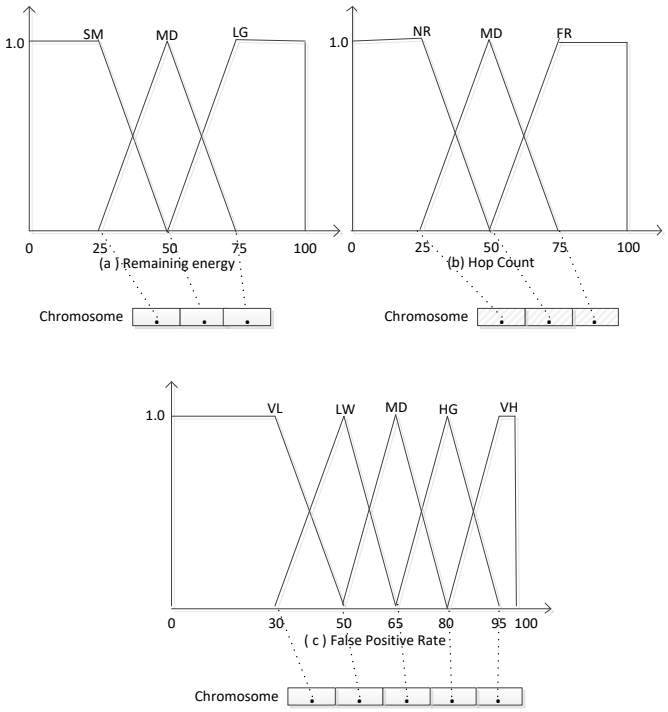


Fig. 2. Genetic representation of the input membership functions.

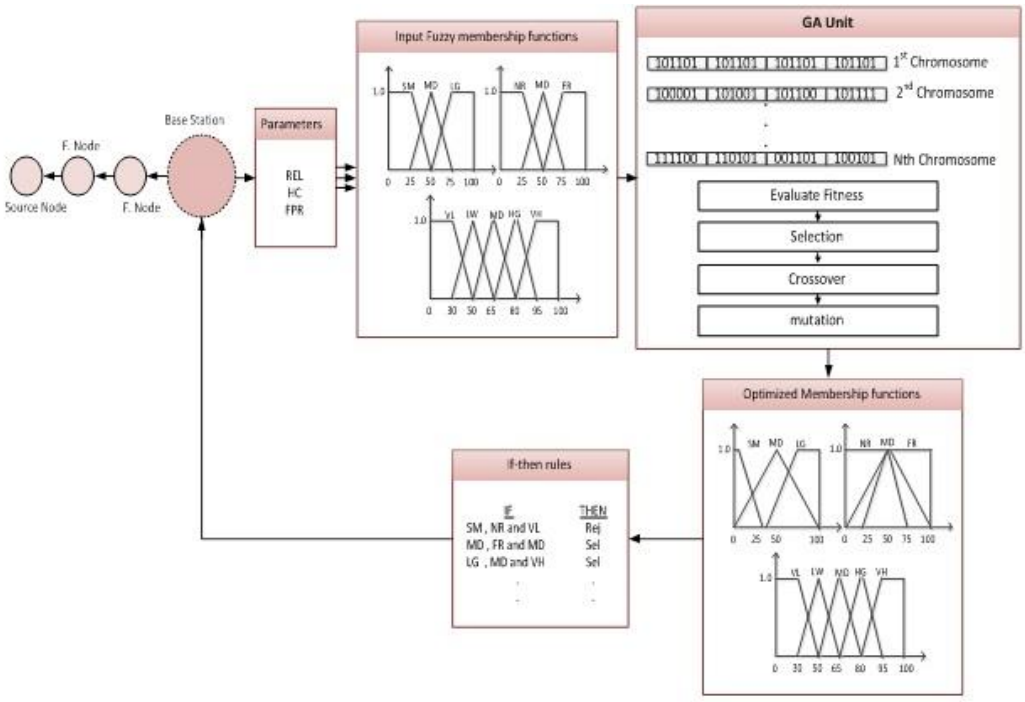


Fig. 3. GA based optimization of fuzzy membership functions

The generated chromosomes are stored in the GA module where each chromosome is represented by the sequence of binary strings. The fitness of the available chromosomes are evaluated in the evaluate fitness segment of the GA module. The chromosomes with high fitness value are selected to generate the children chromosomes through evolutionary techniques employed in the genetic algorithm such as selection, crossover and mutation. The children chromosomes are then selected for the next generation. This way the fitness of chromosomes are gradually increased. This process continues until the optimal chromosomes are generated. The evolution process and its explanation is shown in the fig. 3.

The GA module contains a population of 20 chromosomes in each generation for REL and HC, and a population of 30 chromosomes in each generation for FPR. The simulation runs and regenerates a new population using genetic operations until the terminal condition. Fig. 4 illustrates the optimized input fuzzy membership functions for REL, HC and FPR.

V. Performance Evaluation

The proposed method in a randomly deployed network with 100 sensor nodes is simulated in a custom simulator. The network is comprised of 100 sensor nodes and a base station (BS). The sensor nodes are placed in a 100×100 m^2 and the BS is located at the edge of the network. 66.7 µj and 59.6µj energy is used to transmit and receive a report respectively, and 3.3uj energy is consumed to encode or decode a report. The time off set of nodes is between -3 and +3 unit of time.

To evaluate the performance, we compared the GA based scheme with our previous method (EETF) which was developed to enhance the energy efficiency of TICK based sensor network by selecting most favorite re-encrypting nodes [12].Performance is measured by quantitative metrics of energy dissipation in both the cases, i.e., computational energy dissipation and transmission energy dissipation.

The plot in Fig. 5(a) represent the computational energy consumed in re-encrypting reports when the FPR is 30%. In Fig. 5(b), we measured the computational energy consumed in re-encrypting the reports while the FPR is both variable and increasing with the passage of time. It is shown in Fig. 8(a) that the computational energy consumed in GA based method is less than that of EETF. This is because the membership functions are modified and optimized in our proposed scheme. The computational energy only increases with the increase in FPR.

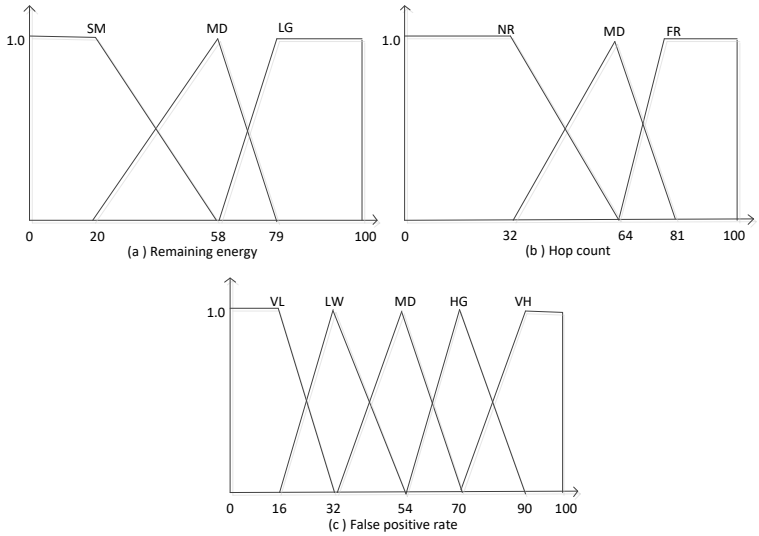
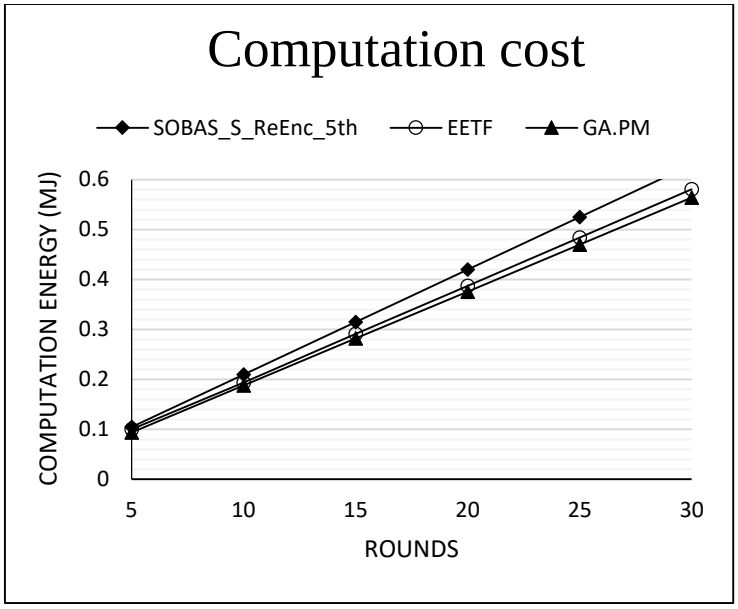
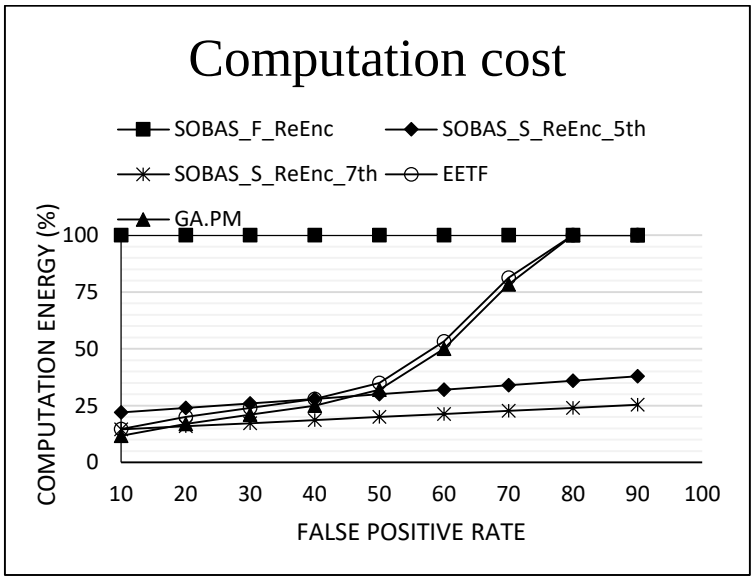


Fig.4. Optimized input fuzzy membership functions



(a) FPR=30%

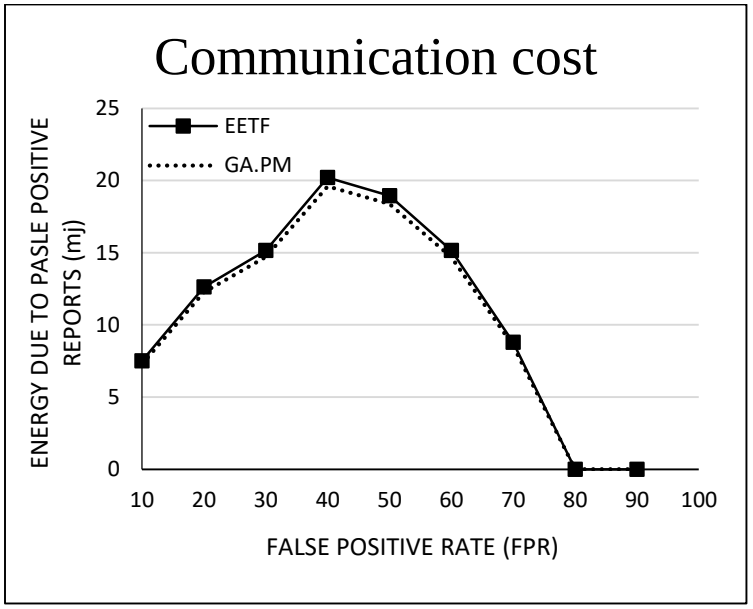


(b) Reports =100

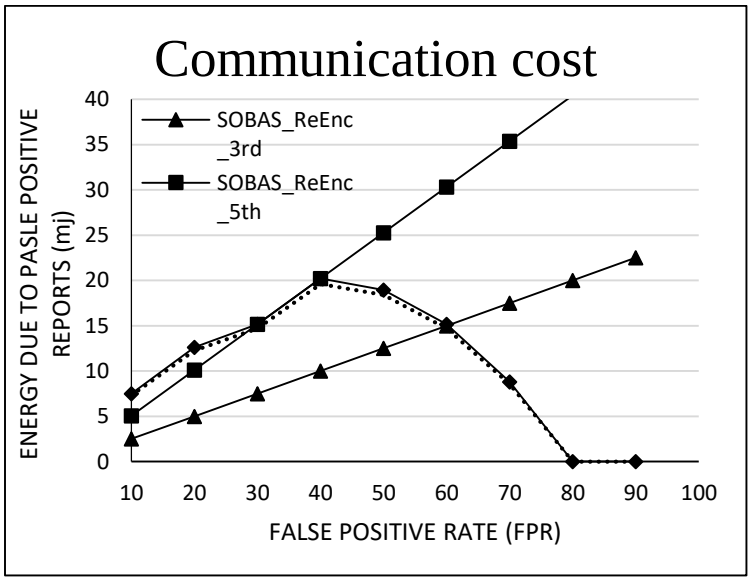
Fig. 5. Computation cost

We also evaluated the communication cost of the EETF and our proposed scheme. GA based scheme reduces the communication cost as membership functions in EETF are optimized and selects most favourite re-encrypting nodes. Fig. 6 (a) and (b) shows the performance of the proposed scheme in terms of communication cost.

Fig. 7 shows the total energy consumption behaviors of the EETS and our proposed scheme. The total energy consumption is comprised of two parts, the computational energy consumption (due to decryption/re-encryption operations) and the communication energy consumption in forwarding the incoming reports from the source node towards the BS due to the false positive rate. The total energy gain in the network is



(a)



(b)

Fig. 6. Communication cost

greater using the proposed method than is possible using EETS. This is because the membership functions are equally important to be optimized. The proposed scheme optimizes the membership functions using genetic algorithm and selects most favourite re-encrypting nodes which reduces the communication cost 2.97% less than that of EETS and improves energy gain.

VI. CONCLUSION

Communication cost in wireless sensor networks is important to be considered because sensor nodes in the network having less computation capacity, stringent energy and limited storage are deployed in hostile environment where an adversary can easily compromise the en-route nodes and inject malicious data in the network. Many en-route filtering schemes have been developed to ensure the security of the network but these schemes employ the exchange of control keying messages techniques and increase the communication cost of the network. Energy Efficiency Enhancement of TICK –based Fuzzy Logic (EETF) in WSNs has been proposed to tackle this issue. Fuzzy membership functions in EETF are not up to the mark and needed to be modified and optimized because optimization of fuzzy membership functions are equally important. In our proposed scheme, we modified amd optimized the input membership functions. As a result, most favourite re-encrypting nodes are selected which reduces the communication cost and false positive rate in the network. Our proposed scheme selected more re-encrypting nodes in the presence of high FPR and few re-encrypting nodes in the presence of low FPR.

VII. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 08, pp.102-114, Aug 2002.

[2] S.R.J Romson and D. J. Moni, "Applications of wireless sensor networks- A survey," Proc. in IEEE Innovations in EEMIT, Fab 2017.

[3] P. Dawal, G. S. Narula, V. Jain and A. Baliyan, "Security attacks in wireless sensor networks: A survey," *Cyber Security (Springer)*, vol. 729, pp. 47-58, April 2018.

[4] T. Kim and H. Lee, "Performance evaluation of the RIX-MAC protocol for wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 2, pp. 746-784, February 2017.

[5] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp.839–850, April 2005.

[6] Yang, H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," *In Vehicular Technology Conference*, vol. 2, pp. 1223-1227, October 2004.

[7] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," *Proc. IEEE Symposium on Security and privacy*, pp. 259–271, May 2004.

[8] C. Kraub, M. Schneider, K. Bayarou and C. Eckert, "Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks," In *2nd Int. Conf. on Availability, Reliability and Security*, pp. 310–317, April 2007.

[9] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, November 2002.

[10] A.S. Uluagac, R. A. Beyah and J. A. Copeland, "Time-based dynamic keying and en-route filtering (TICK) for wireless sensor networks," *Proc. IEEE Global Telecommunications Conference*, pp. 1-6, Dec 2010.

[11] A. S. Uluagac, R. A. Beyah and J. A. Copeland, "Secure source based loose synchronization (SOBAS) for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 803–813, April 2013.

[12] M. Ashraf and T. H. Cho," Energy efficiency enhancement of TICK –based fuzzy logic (EETF) in WSNs," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 9, pp. 4271-4294, September 2018.

[13] M. Akram and T. H. Cho, "Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks," *Ad Hoc Networks*, Vol. 47, pp. 16–25, September 2016.

[14] H. Y. Lee and T. H. Cho, "Fuzzy-Based Reliable Data Delivery for Countering Selective Forwarding in Sensor Networks," In *Proceedings of the 4th international conference on Ubiquitous Intelligence and Computing, Hong Kong*, China, 11–13 July 2007; pp. 535–544.

[15] H. Y. Lee and T. H. Cho, " Optimizes fuzzy adaptive filtering for ubiquitous sensor networks," *IEICE TRANS. COMMUN.*, vol. E94-B, no. 6, June 2011.

[16] M. Akram and T. H. Cho, "A genetic algorithm-based optimized fuzzy adaptive path selection in *wireless sensor networks," SJCMS (Sukkur IBA)*, Vol. 2, no. 1, pp. 1–12, June 2018.

[17] B. Peng and L. Li, "An improved localisation algorithm based on genetic algorithm in wireless sensor networks," *Cognitive Neurodynamics(Springer)*, vol. 9, no. 2, pp. 249–256, April 2015.

[18] S. P. Singh and S. C. Sharma, "Genetic-algorithm based energy efficienct clustering (GAEEC) for homogenous wireless sensor networks," *IETE journal of research*, September 2017.