An Efficient Fuzzy Path Selection Approach to Mitigate Selective Forwarding Attacks in Wireless Sensor Networks

Seyyit Alper Sert*, Carol Fung†, Roy George‡, Adnan Yazıcı*
*Department of Computer Engineering, Middle East Technical University, Ankara, Turkey
{alper.sert, yazici}@ceng.metu.edu.tr
†Department of Computer Science, Virginia Commonwealth University, Virginia, USA
cfung@vcu.edu
‡Department of Computer Science, Clark Atlanta University, Atlanta, USA
rgeorge@cau.edu

***Abstract*—Wireless Sensor Networks (WSNs) facilitate efficient data gathering requirements occurring in indoor and outdoor environments. A great deal of WSNs operates by sensing the area-of-interest (AOI) and transmitting the obtained data to a sink/(s). The transmitted data is then utilized in decision making processes. In this regard, security of raw and relayed data is both crucial and susceptible to malicious attempts targeting the task of the network which occurs on the wireless transmission medium. A node, when compromised, may deliberately forward data packets selectively. When this happens, nodes adjacent to the malicious nodes cannot identify the malevolent node and mitigate the effects of the attacks. In this study, we introduce a fuzzy path selection approach that efficiently mitigates single selective forwarding attacks in WSNs. Performance of our proposed approach and its evaluations are simulated and obtained. Our experimental results show that our approach is an effective solution to serve as a defense mechanism in terms of the efficiency metrics, such as Half of the Nodes Alive (HNA), Total Remaining Energy (TRE), and Packet Drop Ratio (PDR).**

***Index Terms*—fuzzy path selection, selective forwarding, routing security.**

I. Introduction

Wireless Sensor Networks (WSNs), that nowadays consist of thousands of tiny wireless sensing units, became available due to the technological progresses in Micro Electro-Mechanical Systems (MEMS). These wireless sensing units have assorted components such as a wireless antenna, a micro processor, a circuitry for connecting components, different types of sensors per usage purpose, and a power unit [1]. Another advancement has occurred in mobile applications which, together with the propagation of diverse transmission channels [2], has also given birth to the Internet of Things (IoT) concept today. Privacy, security and trust issues become remarkably important due to this changing environment. Security of raw and relayed data should be provided because most WSNs carry out mission-critical tasks, such as health monitoring or surveillance applications. WSNs use the wireless medium for transmission and this results in unique vulnerabilities that are not present in wired networks. The basic problem arises from ineffectively protected wireless medium.

In WSN context, wireless units are expected to be trustful in transmitting data packets to the intended receiver. However, a malicious unit may selectively forward received or obtained packets. This attack type is called *Selective Forwarding (SF)* [3]. In this case, required packets may not reach the intended destination due to a victorious attack. Additionally, nodes that are adjacent to the compromised node hardly identify the attack since packets are forwarded *partially*. This is a hidden problem for mission critical applications that rely on the underlying WSN routing infrastructure. In an effort to address this problem, we exploit the power of Type-I fuzzy sets and introduce a fuzzy path selection approach in order to mitigate SF attacks occurring in WSNs. Our approach seeks to determine a mitigation route among possible candidate routes considering two fuzzy input descriptors. These descriptors are chosen so as to balance the energy consumption of the network and obtained experimental results corroborate the effectiveness of our approach.

The remainder of this study is as follows: in Section II, domain information about SF attack type together with related work are presented. Then, our fuzzy path selection approach is discussed in Section III in detail. Thereafter, our contributions and operation of the methodology are explored by experiments in Section IV and eventually in Section V, we conclude our study and state possible research directions.

II. Background

WSNs substantially deviate from wired systems when security architecture and network layer characteristics are taken into account. Therefore, definitions about security necessities and threat model in this study are depicted in compliance with [4] and [5]. A *secure WSN* should demonstrate security features such as Non-Repudiation, Confidentiality, Freshness/Timeliness, Integrity, Availability, Authentication, Authorization, and Time-Dependent Secrecy. Confidentiality, Integrity, and Availability goals constitute what is often named as CIA triad [6]. These three goals are must for a WSN in order

978-1-5090-6034-4/17/$31.00 ©2017 IEEE

for it to be called as secure. For this reason, integrating these requirements at initial design phase is a desired advantage.

SF attacks are among the routing attacks which take place when packets are routed in the network [7]. In security attack context, there are various routing attacks such as *Sybil Attacks* [8][9], *Sinkhole/Blackhole Attacks* [10], or *Wormhole Attacks* [11][12], when we want to name some. However, due to page restrictions, we will not elaborate into the specifics of these attacks. A comprehensive study on protocol (ZigBee) security structure can be found in [13]. As depicted in these studies, the main weakness in WSNs emerges from the deficiency in securing the transmission medium.

The consequence of SF attacks is the loss of packets without knowing which node/s in the crowd has/have caused the problem. Prior to this study, in our analysis about the impact of routing attacks in [14], we intuitively deduce that defending against selective forwarding attacks may result in more energy consumption and less accuracy in WSN efficiency. This study is the result and addressing of this initial intuition. Many solutions have been proposed so far to defend the network against SF attacks. In the rest of this section, we briefly elaborate a few existing ones in the literature.

In [15], geographic routing [16] approach is combined with watermark-based approach [17] in order to obtain efficiency against SF. A secure routing path is determined by implementing geographic routing and malevolent nodes are isolated by utilizing watermarks. However, energy consumption and transport delays are the drawbacks of this approach. Moreover, the approach is also open to SF attacks occurring in later stages since node/s may be compromised after a secure route setup, which inadvertently falsifies the regular packet delivery ratio.

The approach in [18] is especially appropriate for hierarchical protocols. The mechanism proposes to utilize watchdogs in order to follow up transmission among nodes. These watchers trace the packet rate from adjacent nodes and data is first collected and thereafter analyzed in a probabilistic manner. The problem in this approach lies in the scalability aspect. When the number of nodes increases, there is also a need for increasing the number of watchdogs.

Geethu et al. proposed a multi-path routing [19] which can effectively reduce the chance of packet loss when packets are routed through paths without intersection. In this mechanism, a wireless node eavesdrops on the communication of adjacent nodes. When a packet is dropped, another distinct path is chosen in order to send the remaining packets. This approach can reduce packet drop rate by avoiding malfunctional nodes along the routing path. However, this approach requires nodes to have multiple transceiver units activated, which as a results, augments the consumed energy in the network.

Gulhane et al. proposed to incorporate security into multi-path routing [20]. In this study, MD5 authentication is utilized for identity confirmation and encryption is employed for multi-path security. Nevertheless, implementing encryption in the routing stage can cause excessive cost both before and at the time of data exchange. In addition, there are no simulations or experimental result provided for supporting the proposed mechanisms and algorithms behind them.

In the work of Mathur et al. [21], a sequence number-based SF detection method is proposed. In their WSN routing mechanism, nodes and the sink are using pre-negotiated packet sequence numbers which increase consistently during all packet transmissions. Therefore, a node can easily detect if its neighbor does not forward a packet to the next hop. When a selectively forwarding node is identified, a new path seeking process will be triggered to avoid the SF node for further transmission. However, this method assumes all nodes are able to monitor the transmissions from their neighbor nodes, which may not be the case in most networks.

As stated in the previous paragraphs, there are various studies proposed to defend against SF attacks, however each has its own pros and cons. Data acquisition from sensor nodes and conveying the obtained data towards the desired places are expensive operations regarding the consumed energy in especially the presence of SF attacks. Fuzzy methodologies in this fied have cropped up for the purpose of reducing this excessively consumed energy. Fuzzy processing has drawn attention in research community because of its direct relation with energy-efficiency and relaxation. Now in the next section, we describe our fuzzy path selection procedure which efficiently mitigates SF attacks.

III. Methodology

SF attacks are mitigated by the utilization of a two-phase procedure. In the first phase, compromised node is detected and in the second phase new disjoint routing path is generated by the utilization of fuzzy rules. For the detection phase, we follow the approach as defined in [21] by using sequence numbers with the following features:

- No modification is done on the routing protocol since the data transmission request initiates at any source node when compared to the situation in medical WSNs which is a special case of a general WSN architecture (The sender of RREQ packet is the source node and the sender RREP is the destination node).
- Sequence numbers are appended into the transmitted packets as defined in the original study.

In normal operation, whenever a wireless node has any detection to send to the base station, it sends a RREQ destined to the base station and waits for the RREP packets. According to the received RREP packets, it sets up a route considering the shortest path and initiates data transmission. When an SF attacks occurs, this sender node is unaware of the situation since it has no chance of detection. This is the point which requires the inclusion of the sink. The sink can deduce that the system is under SF attacks by examining the sequence number of received packets. If there is an ongoing SF attack, the received sequence numbers will differ from what it should really be. Here, it is wise to state that this difference can also be the result of bit errors. For this case, a threshold can be set in an effort to distinguish SF attacks from bit errors. However, the discrimination of an SF attack from bit errors

is beyond the scope of this study and if there is a difference between sequence numbers by 5%, we assume that this is only because of a successful selective forwarding attack. When the sink detects the attack, it broadcasts a control packet together with a new RREP packet to the source and initiates the route set-up procedure again. This is where the mitigation process actually commences.

A. System Model

Before explaining the second phase of the proposed mitigation procedure, specifications of the system model that are employed for WSN infrastructure and our assumptions are as follows:

- All nodes (including the base station) are identical, stationary, and deployed randomly.
- The sink and data sender node (the source) are assumed to be trustful.
- All nodes have the same amount of energy initially when they are deployed and the total battery-power of a node is modeled as one (1) joule (j).
- Wireless units are able to tune transmission power according to the distance of the target untis.
- Selective forwarding attack does not occur in a collaborative manner (There can be a single malicious node in the network at any given time).
- Distance between units can be figured out taking the received signal strength into account.

B. Fuzzy Path Selection (FPS) Algorithm

The Fuzzy Path Selection (FPS) Algorithm is designed by taking two crucial factors into account. The first factor is energy-efficiency, and the second one is simplicity in the computational sense. It is a distributed approach since there is no need for the inclusion of sink in order to generate disjoint paths. The sink is only included in the broadcast of control and RREP packets so as to declare the malicious node to the network and initiate a new route set-up procedure by the source node. Motivation behind this approach is to minimize and balance the energy consumption due to multiple transceiver unit activations through an efficient candidate disjoint path generation. FPS considers two fuzzy parameters in the selection of disjoint paths, namely average link residual energy and relative hop count. FPS exploits these parameters with the power of fuzzy logic in calculating the candidate route chance values. With the use of fuzzy descriptors, uncertainties and dominance of a single parameter are handled in a powerful manner when compared to assigning weights to each of them. Operation of the FPS procedure is explained in Algorithm 1 in a pseudo-code manner. Ch_r , AvE_r , and Hc_r represent the candidate chance value, average link residual energy, and hop count a particular route r, respectively.

The detection of an SF attack occurs in the sink, however the actual mitigation process is triggered in the node. Being aware of a SF attack by a control packet, source node starts to collect RREP packet which is broadcast and addressed to itself by the sink. In path selection operation, source node generates

Algorithm 1: FPS Protocol

Input: Route/s (RREP packet/s)
Output: The Mitigation Route (MR)

1 *Th (Threshold value)* $\leftarrow 1$
2 *MR* $\leftarrow$ NULL
3 $Enum(Routes)$
4 **foreach** *route* $i \in Routes$ **do**
5 **if** $[MaliciousNode \in i]$ **then**
6 $Routes \leftarrow Routes - i$
7 **if** *(*$Count(Routes) < Th$*)* **then**
  /* use the same route since there is no other route */
8 $MR \leftarrow CurrentRoute$
9 EXIT
10 **else if** *(*$(Count(Routes) = Th$ **then**
  /* use the single new route */
11 $MR \leftarrow SingleNewRoute$
12 EXIT
13 **else**
14 **foreach** *route* $i \in Routes$ **do**
15 By using fuzzy inputs, generate crisp Ch_i
16 $CandidateRoute_i$ (Id_i, Ch_i, AvE_i)
17 MR $\leftarrow CandidateRoute_1$
18 **for** i = *2 to* $Count(Routes)$ **do**
19 **if** *(*$Ch_i < Ch_{MR}$*)* **then**
  /* do nothing; MR does not change */
20 **else if** *(*$(Ch_i = Ch_{MR})$ *and* $(AvE_i \leq AvE_{MR})$*)* **then**
  /* do nothing; MR does not change */
21 **else**
22 MR $\leftarrow CandidateRoute_i$
23 EXIT

a predefined threshold (*Th*), which is assigned 1 initially. This threshold value is utilized in the Mitigation Route (MR) selection steps. If the number of possible disjoint paths is greater than this threshold (line 13), then fuzzy path selection procedure (line 14-23) commences. Since FPS utilizes average link residual energy and relative hop count in the calculation of chance values, the chance value of each route changes dynamically in FPS due to the varying link energies as the time passes by. Chance value calculation is done by employing defined fuzzy rules to handle uncertainty.

The fuzzy processes are depicted as line number 15 in Algorithm 1 and *Candidate Route* is generated accordingly. The employed fuzzy rules are given in Table I. Rules are evaluated utilizing the Mamdani Controller as a fuzzy inference technique and the center of gravity (COG) method is employed for defuzzification of the output chance values.

There are two fuzzy input descriptors employed so as to calculate the chance values. Average Link Residual Energy is the first of them and Fig. 1 depicts the fuzzy set which defines this variable. The linguistic variables of this set are

low, *medium* and *high*. Membership functions for *low* and *high* variables are trapezoidal functions. However, the membership function of *medium* is triangular.

TABLE I
FUZZY RULES IN FPS ALGORITHM

Average Link Residual Energy	Relative Hop Count	Chance Value
Low	Far	Very Low
Low	Regular	Extra Low
Low	Close	Moderately Low
Medium	Far	Low
Medium	Regular	Normal
Medium	Close	High
High	Far	Moderately High
High	Regular	Extra High
High	Close	Very High

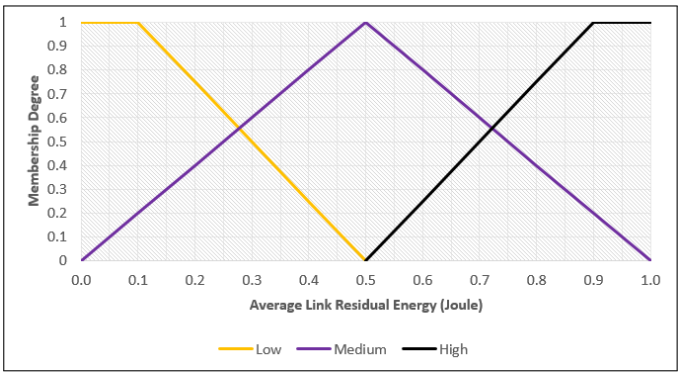

Fig. 1. Fuzzy set describing the fuzzy input variable Average Link Residual Energy.

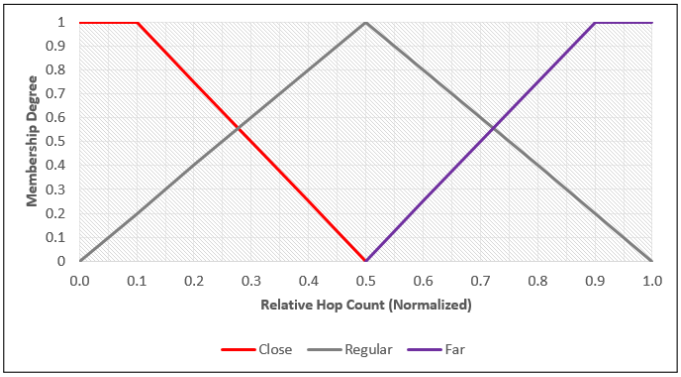

Fig. 2. Fuzzy set describing the fuzzy input variable Relative Hop Count.

The second, and the last, fuzzy input variable is the Relative Hop Count of the candidate route. The fuzzy set which defines this variable is given in Fig. 2. *Close*, *regular* and *far* are the linguistic variables of this fuzzy set. Membership functions for *close* and *far* are trapezoidal functions whereas *regular* has a triangular membership function.

Calculation of the values of Average Link Residual Energy (ALRE) and Relative Hop Count (RHC) of a given route r are given in Eq. 1 and Eq. 2, respectively. As can be seen from the equations, utilization of the average and relative values does not require the inclusion of the sink in the calculation process. This is one of the key factors that makes FPS a candidate mitigation procedure for single SF attacks. In Eq. 2, $max(HopCount)$ value is deduced from the received RREP packets from the source node and utilized in the normalization process of hop counts.

$$ALRE_r = \frac{\sum_{i=1}^{m} RE_i}{m} \tag{1}$$

$$RHC_r = \frac{HopCount_r}{max(HopCount)} \tag{2}$$

Chance value of a received route is the only fuzzy output variable. The fuzzy set employed in describing this fuzzy output variable is presented in Fig. 3. There are nine linguistic variables. *Very Low* and *Very High* have trapezoidal membership functions. The other variables are delineated by employing triangular membership functions. The function in Fig. 3 is preferred after a trial and error process and yielded satisfactory results when utilized.

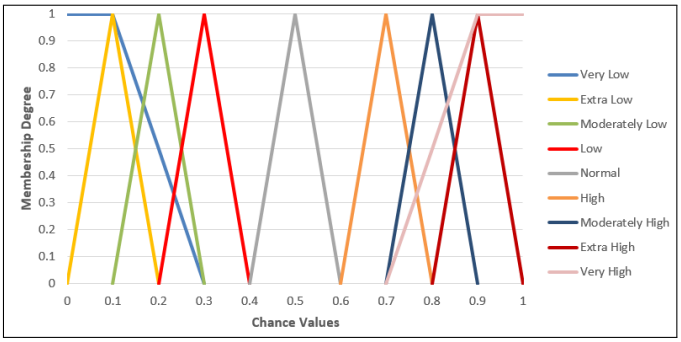

Fig. 3. Fuzzy set defining the fuzzy output variable Chance Value.

Whenever a particular route has little constraint on energy (fuzzy input variable Average Link Residual Energy has the value of *High*) and relatively close to the sink considering the hop count (fuzzy input variable Relative Hop Count has the value of *close*), then it has the maximum chance value (fuzzy output variable Chance Value has the value of *Very High*) to be elected as a Mitigation Route (MR). On the contrary, if the average energy of a particular link is nearly depleted (fuzzy input variable Average Link Residual Energy has the value of *low*) relatively far to the base station (fuzzy input variable Relative Hop Count has the value of *far*) then it has the minimum chance value (fuzzy output variable Chance Value has the value of *Very Low*). The other situations fall between these two extreme cases.

IV. EXPERIMENTAL EVALUATION

In order to analyze the performance of our approach, we conducted a series of experiments on a simulated WSN. In our experimental setting, we set up a sensor network and let a single malicious (compromised) node selectively forward the packets it receives at any given time. Prior to this study, in our

analysis about the impact of routing attacks in surveillance wireless sensor networks [14], we intuitively consider that defending against SF attacks may result in more energy consumption and less accuracy in WSN efficiency. In this section, we corroborate this initial intuition.

A. Simulation Setup

In our experiments, the sensor network is deployed so as to form a rectangular area-of-interest. This is due to its easiness and effectiveness in simulations and it does not have any best or worst case effect on any architecture. Experiments are performed on a 2.70 GHz Intel quad core workstation running the Windows 10 Home operating system with a total of 32 GB DDR4 2133 Mhz RAM, 512 GB RAID-0 SSD Drive. Tests are run 50 times to obtain more reliable results and the average of the results are presented in the evaluation.

Experiments are conducted by using the modified WSN simulator presented in [22]. The simulator is upgraded to utilize the Microsoft.Net Framework 4.5 and modified according to the requirements of FPS algorithm. The sensor network is deployed on a 1000m x 1000m square and consists of 100 randomly deployed nodes. The transmission range is set as 60m. The WSN operates in a non-clustered environment in which each node may send data to the base station either by using a direct or multi-hop transmission. In tested scenarios, the sink and source nodes are trustful and a probability of SF in a compromised node is set as 15%. Since there is no clustering employed for data aggregation, packet size for a wireless node is set to 2000 bits whenever a node sends data to the sink. There is no employed compression on relay nodes.

To be able to efficiently test the impact of SF attacks and analyze the performance of our approach, FPS algorithm is compared with two approaches, the one does utilize any countermeasure to defend against SF attacks, which we call *the baseline*, and the other is the approach in [19]. Half of the Nodes Alive (HNA), Total Remaining Energy (TRE) and Packet Drop Ratio (PDR) metrics are employed for performance measuring. HNA metric depicts the number of round where 50% of all nodes are alive. TRE metric denotes the total remaining energy level of the whole network, calculated by adding the remaining energy levels of each individual node, and utilized for energy-efficiency analysis. PDR metric denotes the percentage of undelivered packets with respect to the total sent packet count.

Representation of the energy dissipation model is as employed in [23] and depleted energy measurement in transmitting or receiving l bit over a distance of d is given in accordance with the first-order radio model. E_{elec} = 50nJ/bit, ε_{fs} = 10pJ/bit/m^2, ε_{mp} = 0.0010pJ/bit/m^4 and d_0 = 20m. E_{elec} is the energy consumption per bit in the transmitter and receiver circuitry and ε_{mp} is the energy dissipated per bit in the RF amplifier.

B. Simulation Results

Table II depicts the obtained results related to HNA and TRE metrics, respectively. According to the results of HNA metric, WSN still pursues a similar same efficient operation when there is no selective forwarding in place. This is because FPS considers Average Link Residual Energy parameter in the selection of retransmission path which balances consumed energy and extend the lifetime of energy-constrained nodes by not retransmitting over them. However, this is not the case for TRE metric. TRE metric decreases in nearly a constant manner since retransmissions consume more reception and more transmission energy. Although, it seems that depleted energy increases, this increase is actually a controlled one since FMS also considers Relative Hop Count in the path selection procedure. In most situations, less number of hops means closer distances from source to destination. By this way, energy-efficient operation is maintained.

TABLE II
OBTAINED HNA AND TRE RESULTS OF THE FPS ALGORITHM.

Algorithm	HNA	TRE(j)
The Baseline	61	18.42
Multi-Path Routing	52	15.19
FPS	56	17.11

Operation of the depicted protocols under single SF presence and their performance considering the number of alive nodes with respect to the time (rounds) are given in Fig. 4. As can be seen from the figure, multi-path routing approach depletes energy much faster than FPS and the baseline. Although FPS suffers from this consumption, it maintains and balances the energy level of the network as much as possible by considering the average link energy in the path selection procedure.

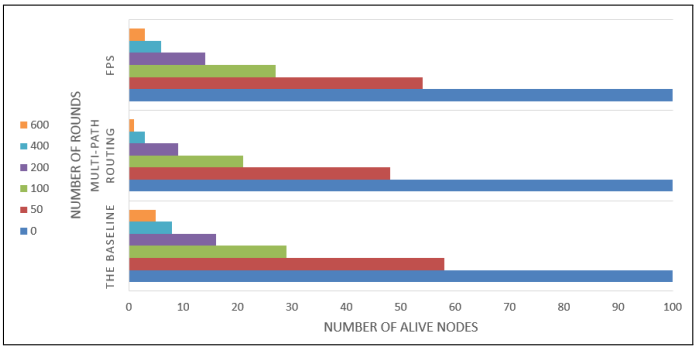

Fig. 4. Operation of the depicted protocols under single SF presence.

TABLE III
OBTAINED PDR RESULTS OF THE FPS ALGORITHM.

Algorithm	PDR (% - First 50 Round)	PDR (% - Total)
The Baseline	11.14	13.23
Multi-Path Routing	8.75	9.66
FPS	6.56	7.48

Obtained results pertaining to PDR metric is presented in Table III. Although FPS algorithm causes a little more energy consumption in order to mitigate an SF attack, this is an

affordable cost. If readily available (current) path can not be utilized for packet transmission due to a compromised node on the relay route, one has to decide whether or not to send data. If the decision is to send data, then the disjoint path should be generated in a wise manner. If the decision is not to send data, then PDR decreases since there is no packet transmission. However in some cases, consumed energy is less important than received packets and for this reason superfluous transmissions occur in sake of successful delivery of data to the intended places. If delivery of data is crucial, like in mission-critical applications, FPS handles this situation effectively.

According to the experimental results, we can deduce that SF has a significant effect over energy-efficiency of WSNs. However, the real cost comes with the shield. The effect of SF becomes significant when there is an implemented countermeasure, such as multi-path routing which causes more energy consumption. Probably the most significant effect of SF over the tested WSN architecture is in the TRE metric since TRE of the network decreases sharply. In case when there is an SF attack and no countermeasure is taken, most WSNs cannot perform its expected operation due to high PDRs causing the WSN to be untrustworthy and restricting its real world usability. For this reason, FPS mitigates SF attacks by consuming little more energy (TRE) when compared to the normal operation maintaining PDR. This makes FPS a candidate SF mitigation approach in wireless sensor networks.

V. Conclusions

Routing security is critical for consistent and effective data transfer in WSNs. However, as a result of unprecedented characteristics of WSNs, it cannot be fully protected from adversaries and selective forwarding is among dangerous and hard-to-detect attack types which targets WSNs that has to be addressed.

In this study, we propose an effective solution which utilizes a fuzzy path selection approach to mitigate selective forwarding attacks in non-clustered WSNs. Our approach efficiently decreases the effects of SF attacks and increase the routing reliability in WSNs. For this reason, it is certainly a candidate approach to be employed as an effective SF defense mechanism.

We believe that future research directions should include lightweight single or colloborative SF defense mechanisms targeting clustered WSN environments and provide multi-objective security solutions.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Vol.38, No.4, pp.393-422, 2002.

[2] H. Zhang, X. Chu, W. Guo, and S. Wang, "Coexistence of Wi-Fi and Heterogeneous Small Cell Networks Sharing Unlicensed Spectrum", IEEE Communications Magazine, Vol.53, No.3, pp.158-164, March 2015.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Vol.1, No.2-3, pp.293-315, 2003.

[4] X.800 : Security architecture for Open Systems Interconnection for CCITT applications, http://www.itu.int/rec/T-REC-X.800-199103-I/e, 1991.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys & Tutorials, Vol.8, No.2, pp.2-23, 2006.

[6] W. Stallings, Cryptography and Network Security-Principles and Practice, 5th ed. Upper Saddle River, NY, Prentice Hall, 2011.

[7] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks", International Journal of Computer Science and Information Security, Vol.4, No.1, 9 pages, 2009.

[8] A. K. Pathan, H. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges", *in Proc.* IEEE 8th International Conference on Advanced Communication Technology, Vol.2, pp.1043-1048, Phoenix Park, 2006.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses", *in Proc.* ACM 3rd International Symposium on Information Processing in Sensor Networks, pp.259-268, California, 2004.

[10] B. J. Culpepper and H. C. Tseng, "Sinkhole intrusion indicators in DSR MANETs", *in Proc.* IEEE 1st International Conference on Broadband Networks, pp.681-688, California, 2004.

[11] S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems", IEEE Transactions on Mobile Computing, No.1, pp.1, PrePrints, DOI:10.1109/TMC.2014.2324572, 2014.

[12] S. Jain and J. S. Baras, "Preventing wormhole attacks using physical layer authentication", *in Proc.* IEEE Wireless Communications and Networking Conference, pp.2712-2717, Shanghai, 2012.

[13] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.40, No.4, pp.419-428, 2010.

[14] S. A. Sert, A. Yazici, and A. Cosar, "Impacts of routing attacks on Surveillance Wireless Sensor Networks", *in Proc.* International Wireless Communications and Mobile Computing Conference (IWCMC), pp.910-915, Dubrovnik, 2015.

[15] Deng H., Sun X., Wang B., and Cao Y, "Selective forwarding attack detection using watermark in WSNs", *in Proc.* of the 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, pp. 109113, Sanya, August 2009.

[16] Yang D., Li X., Sawhney R., and Wang X, "Geographic and energy-aware routing in wireless sensor networks", Int.J. Ad Hoc Ubiquitous Comput., Vol.4, pp.6170, 2009.

[17] Yongliang L.Y.L., Yang X.Y.X., Yao H.Y.H., Huang T.H.T., and Gao W.G.W, "Watermark detection schemes with high security", *in Proc.* of the International Conference on Information Technology: Coding and Computing, Las Vegas, April 2005.

[18] Tiwari M., Arya K.V., Choudhari R., Choudhary K.S. "Designing intrusion detection to detect black hole and selective forwarding attack in wsn based on local information", *in Proc.* the Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 824-828, Seoul, Korea, 2009.

[19] Geethu P.C., Rameez Mohammed A, "Defense mechanism against selective forwarding attack in wireless sensor networks", *in Proc.* the Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013.

[20] Gulhane G. and Mahajan N.V., "Securing multipath routing protocol using authentication approach for wireless sensor network", *in Proc.* of the 4th Int. Conf. on Communication Systems and Network Technologies, pp.729733, Bhopal, April 2014.

[21] Mathur A., Newe T., Rao M. "Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT", Sensors, 16(1), 118, DOI:10.3390/s16010118, 2016.

[22] S. A. Sert, H. Bagci, and A. Yazici, "MOFCA: Multi-objective fuzzy clustering algorithm for wireless sensor networks", Applied Soft Computing, Vol.30, pp.151-165, 2015.

[23] W. Heinzelman, A. Chandrakasan and H. Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks". Proceedings of the 33rd Hawaii International Conference on System Sciences, Vol. 8, Citeseer, pp. 802, 2000.