International Journal on Emerging Technologies **10**(4): 50-56(2019)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

An Efficient Node Ranking Mechanism for Identifying Selective Forwarding Attacks in WSN

Udaya Suriya Raj Kumar Dhamodharan[1], M. Nagamani[2] and V. Krishnamoorthy[3]
[1]Assistant Professor, Department of Computer Science and Engineering,
GGR College of Engineering, Vellore, (Tamil Nadu), India.
[2]Associate Professor, Department of Mathematics,
Global Institute of Engineering and Technology, Vellore, (Tamil Nadu), India.
[3]Associate Professor, Department of Mathematics,
College of Natural Sciences, Arab Minch University, Ethiopia.

(Corresponding author: D. Udaya Suriya Rajkumar)
(Received 07 August 2019, Revised 12 October 2019, Accepted 01 November 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless sensor network has turned in to hot study area owing its extensive variety of use in civilian and military domain, however as it utilizes remote media for communication these are effortlessly inclined to security threats. There are numerous of attacks on wireless sensor networks like Sybil attack, black hole attack, sinkhole attack and selective forwarding attacks. This manuscript focuses on selective forwarding threats. In particular, selective forwarding attacks, attacker nodes perform like ordinary nodes, however, specifically drop packets and the determination of dropping nodes might be random. Recognizing such attacks is exceptionally troublesome and now and then not possible. A trust based detection algorithm called Multi-hop Acknowledgement Detection method is proposed to identify the selective forwarding threat. The detection algorithm is classified into two phases, one is a trust score generation process and another one is an intermediate node-ranking algorithm. The simulation results show that this algorithm has fast convergence and excellent cost performance.

Keywords: Wireless Sensor Network, Selective Forwarding Attack, Trust Based Detection, Packets Drop, Node Ranking, Detection Algorithm.

Abbreviations: DoS, Denial of Service; *SVM*, Support Vector Machine; BS, Base Station; MAC, Media Access Control; WSN, Wirless Sensor Network; NWS, Neighbour Watch Systems.

I. INTRODUCTION

Sensor Networks primary came into renown in the behind 1990s with the beginning of motes device and the petite operating system. Wireless Sensor Networks are modernizing the manner in which the people associate with the real world. They contain of small sensor hubs, which have numerous abilities for example detecting, monitoring, calculation and wireless communications [1]. They are conveyed in enormous amounts to gather information from the environment, perform nearby handling and communicate their results. The basic security issues are to provide confidentiality, integrity, authentication and reliability. To provide secure communications for sensor nodes all messages have to been encrypted and authenticated. It is also responsible for sensing devices and transmission information as well [2].

Threats are classified into two main category, one is an outside Attacker and another is an inside Attacker. An outside attacker may cause eaves drop on data transmission and extended to inject bogus data into the network. Inside attacks are harder to detect and defend against them. It may be compromised sensor nodes and also running the malicious node it will stolen the key material from the legitimate nodes. Based on the nature of the wireless channel modification of information is possible in uncontrolled environment [3]. Inside threats can interrupt the network by alter the packets information this is a vital attack in military application, environment monitoring and other critical infrastructures [23]. Internal attack is very important to analyze the security problem in WSN the intruder node compromised the sensor nodes and learns the crucial information from them. In view of the fact that WSNs having thousands of tiny sensor nodes, the belief concept is execute as a dispersed network where every sensor can assess, store and update, the trueness of further nodes based on the trust model. A detection approach is needed to detect this kind of anonymous behavior within the network. In this manuscript, we examine the Selective Forwarding Attack and its variant, which is extremely easy to execute however hard to detect [24].

These manuscript works illustrate selective forwarding attack in WSN and present a trust based detection algorithm and ranking algorithm to absolutely identify the selective forwarding threat in nodes of the network. The trust based algorithm permit the WSN to choose the majority reliable node in the network. The aspire of the proposed technique to guarantee a consistent information delivery form the WSN to base station.

In selective forwarding, attack the malicious node functions as a regular node yet declines of promote assured selected packets and drop them.

Hence, due to this nature, the selective forwarding attack is very harmful for mission basic applications and can damage the entire network communication, making the system useless. The Introduction section should include the background and aims of the research in a comprehensive manner.

II. MATERIALS AND METHODS

In this part, related works on the identification of Selective forwarding are presented. Here, different strategies to identify the Selective forwarding attack are discussed. Sharma *et al.,* [5], discussed about selective forwarding threat, where wicked nodes act similar to typical nodes and specifically drop sensitive data. The choice of dropping nodes might be arbitrary. Distinguishing such attacks is extremely troublesome and in some cases unimaginable. Cho & Qu [6], presented a selective forwarding with denial-of-service (DoS) attack to improve an improved trust method to identify such attackers and recognize their causalities. Moreover, outline two attackers-aware protocols to redirect fatality node's packets by staying away from the foe. Nithiy & Gomathy [7] demonstrated a flexible packet forwarding method in view of Neighbor Watch System (NWS), to distinguish the malicious conduct of the packet dropper node in the system. The plan works on single-way information sending and changes over into multi-path information endless supply of the founding of victim movement in the system by the NWS. The quantity of multipath relies depends upon the quantity of sub-watch nodes around the victim node. The results of this scheme to make a high success ratio inside the sight of a vast number of packet dropping nodes and accommodates its sending style depending upon the quantity of the dropper nodes on the route to the goal. In author finds a centralized intrusion detection method related to Support Vector Machines (SVMs) and sliding windows [8]. This strategy can identify selective forwarding and black hole threats with lofty exactness without diminish the nodes of their energy.

In author discussed all the past defensive mechanism as indicated by the best knowledge against selective forwarding attack [8]. They likewise classify present techniques as per their character and defense. The nature of a method divided into centralized and distributed design based on recognition and prevention. Hai & Huh [9] demonstrated a lightweight identification technique for neighborhood information. The recognition technique can identify selective forwarding attack with lofty accurateness and slight overhead forced on recognition modules than past works. This plan can distinguish the selective forwarding attack and can likewise manner the malicious node used by the attacker to dispatch the attack. They used the cumulative acknowledgements to be send to the base station when the intrusion is recognized [10]. The overview and investigation of the past strategies to counter selective forwarding attack in WSN. The main goal of the attacker is to prevent the important sensitive data from reaching the base station. To achieve this goal, the malicious node selectively drops certain packets, based on some chosen criteria, and forwards the remaining [11]. The anticipated a defensive procedure which is isolated into three phases: In the first stage the node discovers find a way and its neighbor nodes, in the second stage when the occasion is produced and information is proliferated in multipath and is checked whether the information came to be right or not, and in the last stage if any error is identified then a MONITOR packet is created and the malicious node is expelled. The outcomes have additionally demonstrated that the methodology devour less vitality, good delivery ratio and can avoid delays [12].

Sharmila & Umamaheswari [13] utilized a defensive component based on cumulative acknowledgement utilized to identify selective forward threat in mobile wireless sensor networks. The plan assesses as far as throughput and packet delivery ratio. The malicious node is distinguished taking into account the acknowledgement and energy level of the node. The energy utilization of the discovery plan is less when compared with existing recognition plans.

Singh & Pandey (2014) examined defense scheme against selective forwarding attack utilizing information packet, each node in the sending way sends information packet to individual source node at a fixed interval of time. At the point when the source node gets a data packet from in-between node, it recognizes the malicious node, the source node boycott the malicious and send a new route ask for correspondence [14].

Alajmi & Elleithy (2015) address the protection lapse of WSNs on the network layer, especially selective forwarding attacks. The review incorporates a target for the examination of previous methodologies for taking care of the protection of WSNs on the network layer and their difficulties [15]. Bysani & Turuk, (2011) described specific selective forwarding threats into two classes, one is fall of packets in specific nodes and the other is dropping packets of specific sorts. Three key strategies apply to any malicious node [16].

In showed data provenance oriented technique to identify the threat and the malicious node [17-18]. The plan works in three stages localizing malicious node, identification of attack presence and packet loss detection. The BS (Base Station) for every sensor information flow and after that waits for an adequate number of packet misfortunes starts the procedure. The BS then computes the average packet misfortunate rate and compares it and the common packet loss misfortune to recognize the attack. Upon the identification of attack, the BS alarms the source node and the in between nodes to begin the mechanism of confining the malicious node. Detection of selective forwarding threat in WSN: a survey [19]. In author concentrated on the insider selective forwarding attack [20].

They presented a secure routing protocol taking into account on monitor node and trust method. The character worth is made up with the packet-sending rate and node's lingering vitality. Therefore, this finding and routing mechanism is all common since the fact that it can take assess both the wellbeing and lifetime of the system. They identified selective forwarding threat, which depends on the level of trust and packet failure. In presented a valuable technique for identifying the selective forwarding threat in a heterogeneous sensor network [21]. They utilize dominant high-end sensors and are related to sequential probability ratio test.

III. PROPOSED WORKD

The selective forwarding threat is a critical threat in WSN it is difficult to recognize. This threat is some of the time called a gray hole threat. In an easy appearance of selective forwarding threat, attacker nodes attempts to prevent the packets in the WSN environment by declining to promote or fall the messages going through them. The selective forwarding attack is classified into various types. Fig. 1. Depicted how the selective forwarding attack works through a simple example. The selective forwarding attack may be occurring by way of the connection between Starting node S to Destination node D in between or next node A node and B node. In the pathway to the sink, node S promote or send, the packets to its neighbor node A however node A stop forwarding the packets from node S. Instead of forwarding the packets simply A node can drop the packet. The information from node A does not reach the B node. If not, the node A may perhaps forward the packet to a mysterious malicious node during a high-quality route for eavesdropping.

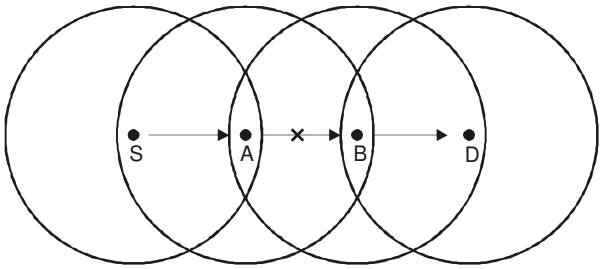

Fig. 1. Selective forwarding attack.

It likewise acts like a black hole in which it declines to promote each packet. The attacker node may promote the packet to the incorrect way, making unfaithful storing data in the WSN [22]. An additional type of selective forwarding threat is known as greed and neglect. In this type, subvert nodes subjectively fail to path a few messages. It can any case take part in lower level protocols and may even recognize the gathering of information to the sender however, it drops sensitive messages arbitrarily. Such a node is careless. When it likewise provide unreasonable needs to its individual particular messages, it is additionally greedy. Besides, an extra conflict of selective forwarding threat is to wait packets going during them, making them confused steering information among sensor nodes. In addition, a further variance of selective forwarding threat is to wait packets available through them, making them the confused steering data in the middle of the wireless sensor nodes.

In solitary kind of the selective forwarding attack, the attacker node can specifically fall the packets originating from a specific node or a collection of nodes. This conduct motive a DOS attack for the specific node or a collection of node appeared in the Fig. 2.

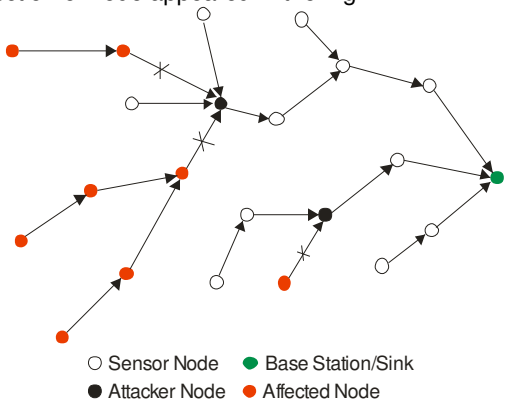

Fig. 2. Selective forwarding attack in form of DoS attack.

Since monitoring the network adds an extra workload to the network, have to consider the characteristics and behavior of the detecting algorithm. The detection algorithm detects the malicious nodes in an efficient manner. If there is any delay in identification of compromised or malicious node, then the other nodes in the network remain in an insecure environment, which may decrease the performance of the network and create congestion within the network. In addition, the last and the most important characteristic of a detection method is that it should produce very less false alarm, which effects or disturbs the innocent nodes within the wireless sensor network. False alarm also produces an extra network overhead. So while designing a detection mechanism, need to consider these characteristics to produce an effective output and detection rate. Considering the wireless sensor network the algorithm must also consider the energy constraint of the network. The cost of executing the algorithm should be very less.

Network Model for Trust based scheme

The proposed trust based detection scheme executes mainly on the base station, thus satisfies the forth characteristics of the detection scheme, less energy consumption in sensor node which work on battery power. The source node promotes the data packets to the base station and assumes that the base station is not limited with its power source. So the proposed detection mechanism executes mainly on the base station. Normally the path between the Source node and destination node is determined and the source node transfers the data packets to the destination node (i.e) base station. While transferring the data packet from the source node to a destination node, information packets may loss due to malicious node.

To prevent such loss, the proposed approach randomly transmits the control packet (Pctrl) which consists of the information about the data packets to be conveyed from source to destination. Every intermediate node for source to destination maintains a packet counter, which gets incremented, when they receive and transmit a packet towards the destination.

Once successful transmission of data, the base station compares the control packet information with the packet counter information. In destination node, packet counter maintains the count of packet received from the intermediates. If the information is mismatched with the destination node, it requests the intermediate nodes to forward the data packet along with their packet counter information is shown in the Fig. 3.

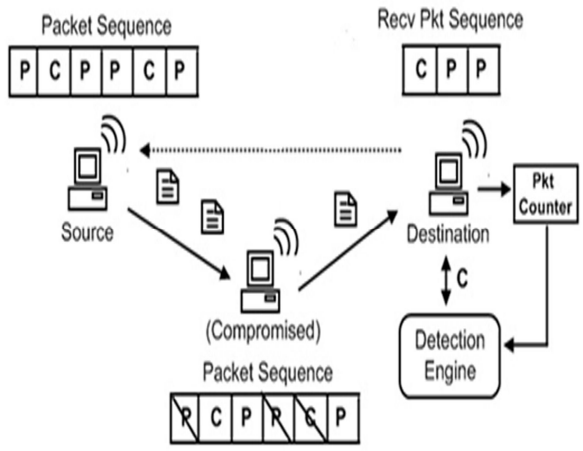

Fig. 3. System modal for selective forwarding attack.

A. Trust score generation process

In trust, score-generating process assumes a network G with N number of nodes. Consider Source node as N_i and the destination node as N_j. For each intermediate node in the source node and destination node as N_i and N_j. The data packet is considered as (P_{data}) and the control packet is (P_{ctrl}) which carries a numerical value (P_{tc}) representing the number of packet transmitted by the source node. These control packets are generated and transmitted in random interval R_v. The source node gets random value R_v using the following Eqn. (1).

$$R_v = R \text{ and } (R_{min}, R_{max}) \quad (1)$$

where, R_{min} and R_{max} is the minimum and maximum value of R_v respectively. For each N round the destination node fetches the packet counter information (P_{data}) and the (P_{ctrl}) from the intermediate node. Having the in between node information the destination node calculate the node was suspicious or not is shown in the below Eqn. (2) and (3).

Data Packet (P_{data} n Control Packet (P_{ctrl}) ≠ 0 (2)

Data Packet (P_{data}n Control Packet (P_{ctrl}) = 0 (3)

If the condition satisfies the equation (2) the node was suspicious, otherwise the node was genuine node.

Algorithm for trust score generation process

Step 1: Consider the wireless sensor network G.

Step 2: G consists of N number of nodes G = (N_1, N_2, N_3, N_4,…….N_m).

Step 3: In a Considered path of nodes assign N_i as (Source node) and N_j as (Destination node).

Step 4: From N_i to N_j the data packet (P_{data}) and Control Packet (P_{ctrl}) is getting transmit.

Step 5: For each round the (P_{data}) and (P_{ctrl}) information is updated in the information table.

Step 6: If (N_i (P_{data} & P_{Ctrl} (T_P))-N_j (P_{data} & P_{Ctrl} (R_P)=0)

Step 7: Node is considered as genuine node.

Step 8: Else

Step 9: Node is suspicious

Step 10: End

B. Intermediate Node Ranking Method

The intermediate node ranking method is used to generate a trust score calculation of each intermediate node. Here, the system considers the source and destination as genuine nodes. Both processes are done in multiple rounds. The detection starts only when the destination's counter is mismatched with the value extracted from the control packet, which carries a numerical value representing the amount of packets transmitted by the source node. Here, T_P represents the total packet transmitted and represents the total received packet R_P. After this we use an intermediate node ranking method to find the selective forwarder from the given Eqn. (4).

$$R_{\text{score}} = \frac{\sum TP}{\sum P_{Rp}} \quad (4)$$

The intermediate node ranking method used in this system is based on the heuristic technique (i.e.), if a node is identified a number of times, it is as suspiciously a bad node. We can find out the set of suspicious nodes after *n* steps of detection. A suspicious node is sorted in the decreasing order of their trust score. The bad node will be identified because of highest value chosen and all the pairs that contain this node are removed resulting in new sets.

C. Simulation result

The simulation was performed on the Ns-2 simulator and the maximum number of nodes considers for computation purpose is 200 nodes. An AODV routing algorithm is considered for data packet transmission. The parameters used for simulation purpose are presented in Table 1.

Table 1: Simulation Parameters for selective forwarding.

Network Dimensions	1400 m × 700 m
Number of Nodes	200
Size of Packets	512 bytes
Application Traffic	CBR
Radio propagation model	Two ray ground
Routing Protocol	AODV
Type of Attack	Selective Forwarding
Channel Type	Wireless channel
MAC Type	802.11

Network for simulation is shown in Fig. 4, here node 23 is the source node and the node 50 is base station or destination node.

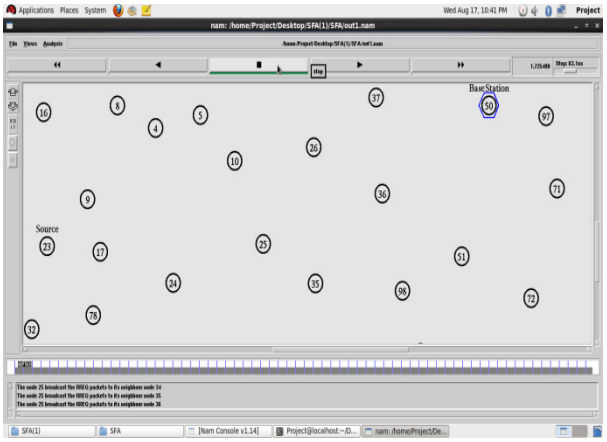

Fig. 4. Initialization of source node and destination node.

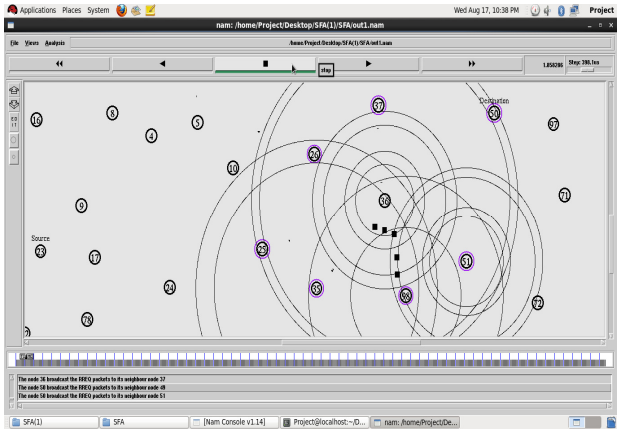

Fig. 5. Packet drop process in the intermediate nodes.

Fig. 5 shows the packet drop process in the intermediate nodes when communication happens between source node to the destination node. The packet drop occurs in some intermediate nodes are node 26 and node 37.

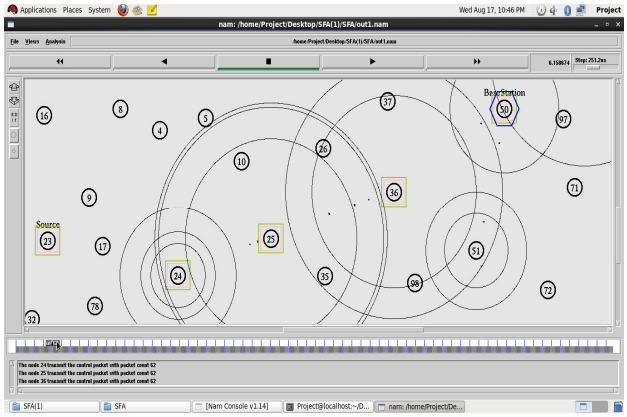

Fig. 6. Communication between source to destination node.

After identifying the malicious node using proposed approach, choose an alternate and secure path the data can be transmitted through intermediate nodes. And the communication between source node 23 to the destination node 50 by considering intermediate nodes of node 24, node 25 and node 36 is depicted in Fig. 6.

IV. RESULTS AND DISCUSSION

In Fig. 7 shows the packet delivery of the existing trust defence scheme and proposed trust based scheme. Here, the numbers of nodes are 200. From the simulation results, it is shown that the packet delivery ratio in the existing trust defence scheme is 0.962 but in proposed trust based scheme is 0.978 for 50 nodes. Likewise, for 100 nodes, the packet delivery ratio in the existing trust defence scheme is 0.968 but in proposed trust based scheme is 0.982. For 150 nodes, the packet delivery ratio in the existing trust defence scheme is 0.972 and in the proposed trust defence scheme is 0.989. For 200 nodes, the packet delivery ratio in the existing trust defence scheme is 0.978 and in proposed trust based scheme is 0.990.

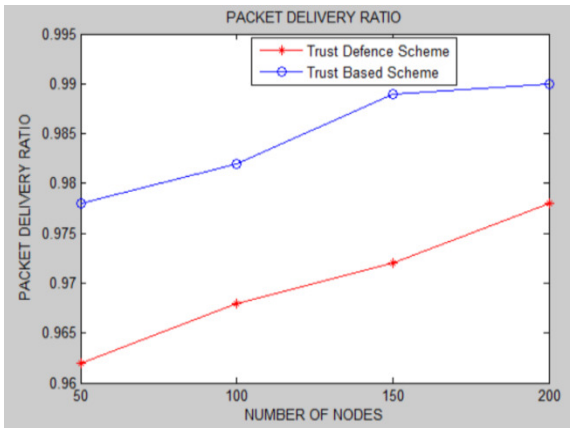

Fig. 7. Comparison of trust defence scheme with trust based scheme.

Fig. 8 shows the average delay of the existing trust defence scheme and proposed trust based scheme. Here, the numbers of nodes are 200. From the simulation results, it is shown that the average delay in the existing trust defence scheme is 17.95 but in proposed trust based scheme is 12.02 for 50 nodes. Likewise, for 100 nodes, the average delay in the existing trust defence scheme is 17.69 but in proposed trust based scheme is 12.02. For 150 nodes, the average delay in the existing trust defence scheme is 20.27 but in the proposed trust defence scheme is 6.03. For 200 nodes, the average delay in the existing trust defence scheme is 22.64 and in proposed trust based scheme is 6.02. Compare with existing mechanism the average delay was lesser in the proposed detection scheme; it shows the efficiency of the proposed algorithm.

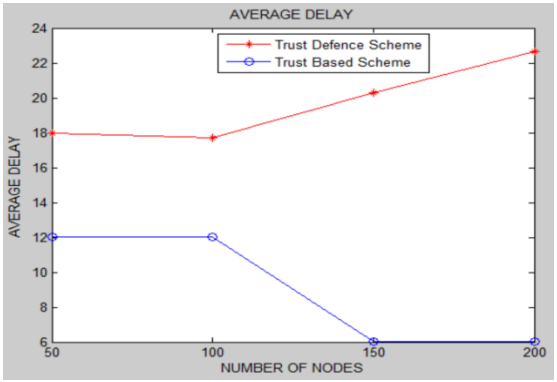

Fig. 8. Comparison of trust defence scheme with a trust based scheme.

Fig. 9 shows the throughput of the existing trust defence scheme and proposed trust based scheme. Here, the numbers of nodes are 200. From the simulation results, it is shown that the throughput in the existing trust defence scheme is 59.62 but in proposed trust based scheme is 75.03 for 50 nodes. Likewise, for 100 nodes, the throughput in the existing trust defence scheme is 69.12 but in proposed trust based scheme is 77.02.
For 150 nodes, the throughput in the existing trust defence scheme is 71.14 but in the proposed trust defence scheme are 84.03.

For 200 nodes, the throughput in the existing trust defence scheme is 74.30 and in proposed trust based scheme is 94.04. Compare with existing mechanism, throughput is higher in the proposed detection scheme its shows the efficiency of the proposed algorithm.

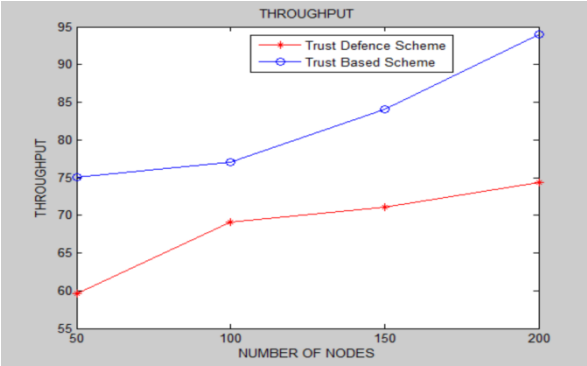

Fig. 9. Comparison of throughput with trust defence scheme with trust based scheme.

Fig. 10 shows the routing overhead of the existing trust defence scheme and proposed trust based scheme. Here, the numbers of nodes are 200. From the simulation results, it is shown that the routing overhead in the existing trust defence scheme is 0.110 but in proposed trust based scheme is 0.037. Likewise, for 100 nodes, the routing overhead in the existing trust defence scheme is 0.150 in proposed trust based scheme is 0.053. For 150 nodes, the routing overhead in the existing trust defence scheme is 0.170 but in the proposed trust defence scheme is 0.075. For 200 nodes, the routing overhead in the existing trust defence scheme is 0.180 but in proposed trust based scheme is 0.115. Compared with the existing mechanism [14]. The routing overhead is less in the proposed detection scheme.

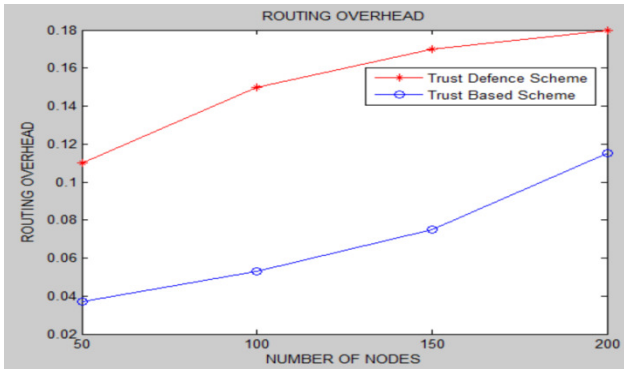

Fig. 10. Comparison of routing overhead with trust defence scheme vs trust based scheme.

V. CONCLUSION AND FUTURE SCOPE

The selective forwarding attack is a kind of attack in the inside of WSN in which a malicious node can drop the packet. The basic need of the network is to detect the type of attack. In this work, a trust based detection scheme with intermediate node ranking technique was proposed for identifying selective forwarding attacks. Distinct other general methods in which recognition is a continuous process, the proposed scheme acts only when it finds the counter mismatch in the destination. The consequence of the proposed approach was assessed utilizing a few parameters like throughput, average delay; throughput and routing overhead are enhancing the execution of the WSN environment. In future, this work can further be stretched out by analyzing performance parameters and implementing it with ongoing application of WSN and also in different IOT devices with intelligent concepts.

ACKNOWLEDGEMENTS

The Topic was the part of the research work of D. Udaya Suriya Rajkumar, Sathyabama University, Chennai.

Conflict of Interest. No Conflict of Interest.

REFERENCES

[1]. Agrawal, S., Jain, S., & Sharma, S. (2011). A survey of routing attacks and security measures in mobile ad-hoc networks. *Journal of Computing*, Vol. *3*(1): 41-48.

[2]. Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and counter measures. *Journal of Network and computer Applications*, *35*(3), 867-880.

[3]. Olakanmi, O. O., Pamela, A., & Ashraf, A. (2017). A review on secure routing protocols for wireless sensor networks. *International Journal of Sensors Wireless Communications and Control*, *7*(2), 79-92.

[4]. Malik, R., Sehrawat, H., & Singh, Y. (2017). Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science*, *8*(5), 1835-1838.

[5]. Sharma, P., Saluja, M., & Saluja, K. K. (2012). A review of selective forwarding attacks in wireless sensor networks. *International Journal of Advanced Smart Sensor Network Systems*, *2*(3), 37-42.

[6]. Cho, Y., & Qu, G. (2013). Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs. *International Journal of Distributed Sensor Networks*, *9*(8), 1-16, ID 205920.

[7]. Nithiy. S., & Gomathy. C. (2018). An Investigation on Security Attacks in Wireless Sensor Networks. *International Journal of Pure and Applied Mathematics*, Vol. *119*(15), 927-935.

[8]. Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information* (pp. 335-340) Melbourne. IEEE.

[9]. Hai, T. H., & Huh, E. N. (2008). Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge. In *2008 Seventh IEEE International Symposium on Network Computing and Applications,* NCA'08, Cambridge, (pp. 325-331). IEEE.

[10]. Kim, Y. K., Lee, H., Cho, K., & Lee, D. H. (2008). CADE: Cumulative acknowledgement based detection of selective forwarding attacks in wireless sensor networks. In *2008 Third International Conference on Convergence and Hybrid Information Technology* (Vol. 2, pp. 416-422). IEEE.

[11]. Singh, B. (2014). Security Mechanism for Selective Forwarding Attacks in Wireless Sensor Networks: Review and Analysis. *IOSR Journal of Computer Engineering*, Vol. *16*(14), 7-13.

[12]. Parida, A., Tarasia, N., & Patnaik, T. A. (2012). Security against Selective Forward Attack in Wireless Sensor Network. *IOSR Journal of Engineering*, *2*(5), 1200-1206.
[13]. Sharmila, S., & Umamaheswari, G. (2012). Defensive Mechanisms of Selective Forward Attack in Wireless Sensor Networks. *International Journal of Computer Applications*, *39*(4), 43-49.
[14]. Singh. H., & Pandey, V. (2014). A Defence Scheme to Detect Selective Forwarding Attack in WSN. *International journal of advanced research in computer science and software engineering*, Vol. *4*(8), 539-545.
[15]. Alajmi, N. M., & Elleithy, K. M. (2015). Comparative analysis of selective forwarding attacks over Wireless Sensor Networks. *International Journal of Computer Applications*, *111*(14). 27–38.
[16]. Bysani, L. K., & Turuk, A. K. (2011). A survey on selective forwarding attack in wireless sensor networks. In *2011 International Conference on Devices and Communications (ICDeCom) Mesra,* 1-5. IEEE.
[17]. Zhang, Q., & Zhang, W. (2019). Accurate detection of selective forwarding attack in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *15*(1), 1-8.
[18]. Khan, W. Z., Yang, X., Aalsalem, M. Y., & Arshad, Q. (2011). Comprehensive study of selective forwarding attack in wireless sensor networks. *International Journal of Computer Network and Information Security*, *3*(1), 1.
[19]. Shirley, J. A., & Jose, J. J. R. (2014). Detection of selective forwarding attacks detection in Wireless Sensor Networks: A Survey. *International Journal of Scientific Engineering and Research*, Vol. 2(6): 48–51.
[20]. Dubey, O. & Kumar, G. (2018). Solution to Selective Forwarding Attack in Wireless Sensor Networks. *International Journal of Student Research in Technology & Management*, Vol. *6*(2): 25-30
[21]. Brown, J., & Du, X. (2008). Detection of selective forwarding attacks in heterogeneous sensor networks. In *2008 IEEE International Conference on Communications* (pp. 1583-1587). IEEE.
[22]. Hu, Y., Wu, Y., & Wang, H. (2014). Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN. *Wireless Sensor Network*, *6*(11), 237-248.
[23]. Udaya Suriya, R.D. and Rajamani, V. (2013). A leader based monitoring approach for sinkhole attack in wireless sensor network. *Journal of Computer Science*, Vol. *9*(9): 1106-1116.
[24]. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, Vol. *10*(1155): 1-7.

How to cite this article: Dhamodharan, U. S. R. K., Nagamani, M. and Krishnamoorthy, V. (2019). An Efficient Node Ranking Mechanism for Identifying Selective Forwarding Attacks in WSN. *International Journal on Emerging Technologies*, *10*(4): 50–56.