SESCAS: A System for Mitigating Forwarding Misbehaviour in Wireless Sensor Networks

Premkumar. M, Sundararajan. TVP, Bhuvaneswari. A, Bhuvaneshwari. M, Deepika. S

Abstract*: Remote Sensor arrange is the most standard administrations utilized in business and modern applications because of its specialized advancement in the processing, communication and low-control utilization of installed PC equipment. Due to open sent nature, the attackers effectively attack the node, so there is an absence of security. To avoid this, Selective sending approach is actualized. This paper aims to establish a simple countermeasure Scalable and Energy efficient Single Check Point based Acknowledgement Scheme; SESCAS is to detect and isolate the misbehaviour node in a wireless sensor network based on time out and retransmission. We carry out extensive simulation experiments to evaluate and compare performance with the extensive CHEMAS, CAM and CAD. The result of the simulation shows that the proposed mechanism can diminish the false recognition rate, collision of packets, energy utilization rate, propagation delay; we likewise enhance the packet delivery ratio and identification rate.

***Index Terms*: Check point detection, Forward misbehaviour, Software Cluster based Management, Wireless sensor network.**

I. INTRODUCTION

A wireless sensor network (WSN) is a network which consists of many low powered devices that are spatially deployed to supervise the environmental conditions in hostile areas. These gadgets, or nodes, when combined with routers and a gateway, give rise to a typical WSN system. These distributed nodes will communicate wirelessly to a central gateway. It provides a link between the wired world and them to collect, process, evaluate, and present the data. To extend distance and improve the reliability in a WSN, the routers can be used to gain an additional communication link between end nodes and the gateway. Currently, the WSNs are ready to be deployed at an accelerated pace. This new technology is exciting with unlimited potential for numerous application areas including environmental monitoring, medical applications, transportation, crisis management, homeland defence, entertainment and smart spaces.

Since, nodes of WSNs are exposed to different environmental factors during deployment stage and are often left unprotected during communication, this make them vulnerable to attacks. When sensor network are deployed in hostile environments security becomes more important as they are prone to different types of malicious attacks [16] & [22].The attacker easily attacks the nodes and retrieves the data or even change the data due to its open nature. Most of the networks routing protocol are not suitable for security purpose. WSNs are easily attacked by the popularly-known denial of service attack (DoS) [15] that mainly target the availability of services by interrupting network routing protocols or interfering with currently running communications. Selective forwarding attack means disruption in packet transmission due to the unfortunate invitation of one or more malicious nodes in the communication path. In selective forwarding attack, dropping of packets takes place due to the malicious node in the network. This malicious node does not allows the forwarding of the packet to the sink [14]. This type of selective forwarding attack drops the packet from the nodes in a random manner. In black hole attack [1] & [11], whereby an infected node drops any incoming packet without letting the communication parties have knowledge about it (blindly), is a problem that needs greater attention to address forwarding misbehaviour issues aroused due to such nodes.

In order to provide security for sensor network, various types of key management techniques are applied. Due to this attack, adversaries cannot forward the certain messages and simply drop them. This leaves the attacker to stick to an option to use a malevolent device to create a huge number of entities in order to gain influence in the network traffic. The ID of these malevolent nodes can be the result of forged network additions or duplication of existing legitimate identities. The attack especially Sybil targets fault tolerant schemes including distributed storage, topology maintenance, and multi-hop routing and it leads to data loss.

II. RELATED WORKS

In this paper, the selective forwarding misbehaviour is overcome [3], [11-13] & [21], which means the malicious node in the network, deny the forwarding packets and selectively drop the packets and lack of security in the network. This mainly affects the forwarding packet transmission efficiency. To overcome this, in the network, the neighbouring node will intimate the previous node regarding failure and then it decides to change the path. Then the packet follows the alternate path which means shortest path. The remaining packet is forwarded to the destination as it is. This leads to reduction in the fake recognition rate and improve packet transport efficiency.

Revised Manuscript Received on July 05, 2019.

Premkumar. M, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.

Sundararajan. TVP, Department of ECE, Sri Shakthi institute of Engineering and Technology, Coimbatore, India.

Bhuvaneswari. A, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.

Deepika. S, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.

Bhuvaneshwari. M, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India.

This also limits the wrong detection of the malicious node. To overcome this, the detection of vicious node is proposed and isolates the node from the network and also increase the energy consumption in WSN.

We propose a unit checkpoint based detection method, known as SESCAS, in WSNs. The earlier schemes [2]-[5], different checkpoint nodes are considered in the network for more accurate detection of the malicious node. The SESCAS scheme implements the cluster head management, alarm packet and alternate shortest path in the network.

The diligent scheme called SESCAS is proposed which expresses analytical outcome for false recognition rate. The earlier schemes based on checkpoint based detection monitor called CHEMAS [3], SCAD [1] and CAD [4] is also referred which improves the data security in WSN in our execution.

III. SESCAS FRAMEWORK

A. System Model

Node clusters are designed in such a way that the lowest energy consumption takes place in a wireless sensor network. In heterogeneous networks, Weight Based Clustering technique is adopted. The framework chooses the better cluster heads thereby increasing the lifetime and throughput of WSN through efficient clustering algorithm [20]. Also, clustering increases the scalability and network life span. This distribution control over the network is to make cluster head more diverse. It increases the life span by distributing load by making intelligent decision. Nodes having high energy are allocated more loads thus increasing the lifetime of the network. The clustering provides the shortest path to travel the information. Only cluster heads communicates with the other cluster head thus reducing the data redundancy which usually happens when each node perform its own data aggregation and transmission [10] function separately. This algorithm provides very efficient way of communication in sensor networks when a centre point has the ability to differentiate a present event, it changes into a source centre, which produces a data package, and transports the package toward a sink in WSNs [17]. To pass on the user data package toward the sink, an essential convey based sending [6], composed scattering [7], or then again geographic-based directing [8] frameworks can be sent. Each centre point thinks about its one-hop neighbour centre points by exchanging a one-time single-bounce Hello divide with its centre id [6].

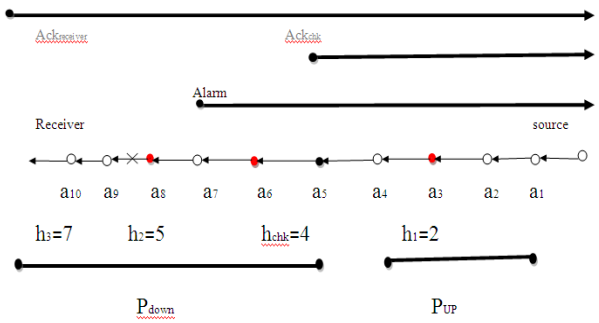

Figure 1. SESCAS network model.

The framework is thick enough to find various sending contender centre points. Thus, a singular centre point interfacing two sub networks isn't considered in light of the way that it could be a single reason for frustration or a vindictive centre point. A fundamental motive of the enemy is to attack advantage openness moreover, spoil the framework execution by interfering with on-going trades. An adversary can catch and deal a true centre point to continue maliciously.

A defective centre node can interfere with the on-going communication and may explicitly drop the content rich packets moving toward package to daze a sink. The malevolent centre point may similarly tune in an on-flying pack and import false information or modify its bundle header to hoodwink orchestrate traffic. Despite, if a sender can affirm a bundle with a light-weight propelled stamp [9], a recipient can without quite a bit of a stretch check the bundle and recognize any change. In this paper, the explicit sending ambushes or the poorly arranged circumstances [2] – [5] that can't be distinguished by mechanized imprints and cryptographic locals is discussed.

B. Single checkpoint-Based Detection

In this approach, nodes are made in a Network .One of the hub is considered as the source node. The source hub conveys the data to the sink. In this the Intermediate hub is considered as the checkpoint node. After each data packets, sent to the node, the hubs send the acknowledgement to the checkpoint hub and the checkpoint hub gets the acknowledgement and intimate to the source node. The source hub gets the quantity of acknowledgement as equivalent to the quantity of nodes. If the acknowledgement isn't sent to the source node, then the hub is considered as the malicious node. Due to this malicious node, the packet drop happens in the network. An additionally significant issue is the packet delay that occurs in the WSN [19]. To keep away from this, the below mentioned strategy is followed. The clock is set for every data packets. In the hub, the time is set and within the time the alarm is sent to the source node. This prompts the decrease of propagation delay. The false detection rate is additionally reduced. The source hub retransmits the data packet and recognizes the malicious hub by methods for ACK. Then again retransmission takes place. Finally the malicious node is isolated.

Vitality reaping hubs are made for transmission of information packets [18]. Due to this vitality utilization takes place. And likewise no bundle drops happen because of the vitality collecting node. Higher recognition rate because of the checkpoint hub approach. False discovery rate is countermeasure due to the particular forwarding way.

C. Detection Analysis

The maximum waiting period is estimated using a single-hop based propagation travel time (P_{TT}). It can be measured by time between a node transmits the information ($S_{T,Info}$) and it receives an acknowledgement from the tagged nodes or the destination ($R_{T,Ack}$).

The P_{TT} is divided by the number of hop count from the node to the checkpoint or

the sink which is denoted as N_k . The low pass filter with gain constant α is used to update the P_{TT} .

$$P_{TT} = \alpha . P_{TT} + (1-\alpha) . P_{TT,k-1} ---(1)$$

Where $P_{TT,k-1}$ is most recently received acknowledgement packet which is denoted as

$$P_{TT,k-1} = \frac{R_{T,Ack} - S_{T,Info}}{N_{k-1}} ---(2)$$

Thus the maximum waiting period is

$$T_{MW} = P_{TT} . N_k + N_k . \delta ---(3)$$

Assume that the false detection rate (F_{DR}) which is the sum of average false detection rates of information (F_{DRI}), Acknowledgement (F_{DRA}) and the Alarm (F_{DRM}) packet losses. The F_{DR} is denoted as

$$F_{DR} = F_{DRI} + F_{DRA} + F_{DRM} ---(4)$$

The F_{DRI} is denoted as

$$F_{DR} = \frac{1}{n-m-1}(F_{DR1} + F_{DR2}) ---(5)$$

Where

$$F_{DR1} = \sum_{i=1}^{m} \sum_{j=0}^{N_i - N_{i-1} - 2} (1-\varphi)^{2j+2N_{i-1}} \varphi ---(6)$$

$$F_{DR2} = \sum_{j=0}^{n-N_m-2} (1-\varphi)^{2j+2N_m} \varphi ---(7)$$

Here, $N_i \ (0 \le i \le m, N_0 = 0)$ is the number of hops between the first node and i^{th} adversary node.

The false detection rate in terms of acknowledgement F_{DRA} can be expressed as

$$F_{DRA} = F_{DRA1} + F_{DRA2} ---(8)$$

$$F_{DRA1} = \frac{RD_{CP}}{N_{CP}} (F_{DRA1,1} + F_{DRA1,2}) ---(9)$$

Where

$$RD_{CP} = (1-\varphi)^{N_{CP}} ---(10)$$

$$F_{DRA1,1} = \sum_{j=0}^{N_{CP}-N_k-1} (1-\varphi)^{N_{CP}-1} \varphi ---(11)$$

$$F_{DRA1,2} = \sum_{i=l}^{1} \sum_{j=0}^{N_i - N_{i-1} - 2} (1-\varphi)^{N_{CP}-1} \varphi ---(12)$$

Similarly

$$F_{DRA2} = \frac{RD_{DT}}{n-m-1} (F_{DRA2,1} + F_{DRA1,2}) ---(13)$$

Where

$$RD_{DT} = (1-\varphi)^{n-1} ---(14)$$

$$F_{DRA2,1} = \sum_{j=0}^{n-N_k-1} (1-\varphi)^{n-2} \varphi ---(15)$$

$$F_{DRA2,2} = \sum_{i=p}^{1} \sum_{j=0}^{N_i - N_{i-1} - 2} (1-\varphi)^{n-2} \varphi ---(16)$$

The false detection rate in terms of alarm F_{DRM} can be denoted as

$$F_{DRM} = \frac{1}{n-m-1} (F_{DRM1} + F_{DRM2}) ---(17)$$

Where

$$F_{DRM1} = \sum_{i=0}^{n-2} (1-\varphi)^{2i-1} \varphi^2 ---(18)$$

$$F_{DRM} = \sum_{i=1}^{m} (1-\varphi)^{2N_i - 1} \varphi^2 ---(19)$$

IV. PERFORMANCE EVALUATION

The Network Simulator (NS) is a discreet event openware simulator which are targeted at networking research and provides the substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks. Table I show the various evaluation parameters which are used in the simulation environment.

Table I Evaluation parameters

Sl. No	Specification	Value
1	Simulation space	1000x1000m
2	Simulation time	1000s
3	Node coverage range	15m
4	Node ID	16 bit
5	Packet size	1 Kbytes
6	Packet drop rate	10-20%
7	No. of nodes	200
8	No. of attack nodes	01-Jun
9	Message interval time	0.02s
10	Radio data rate	250kbps
11	Channel error rate	0-8 %
12	Radio Model	CC2420
13	Node energy	100J

• Packet Delivery Ratio: The packet delivery ratio is the ratio of packets successfully received to the total packets sent. Throughput is the frequency at which information is sent through the network.

- False Detection Rate: Watchdog resides in each node and is based on extra-listening activities. Through overhearing, each node can detect the malicious action of its neighbours and report other nodes. So some advantages with this mechanism are: minimized false detection rate and less overhead on the network traffic.
- Packet drop rate: Packet drop rate means number of packets received at the destination lesser than the number of packets sent at the source. Due to Packet loss, the network efficiency is reduced. The main factor of packet loss is the multipath forwarding path.
- Energy Consumption: A WSN consists of many sensor nodes which sense physical phenomena or collect data from an environment. Some parameters such as position, distance and power consumption for each node and communication technology between sensor nodes have inevitable impact over the network's performance.

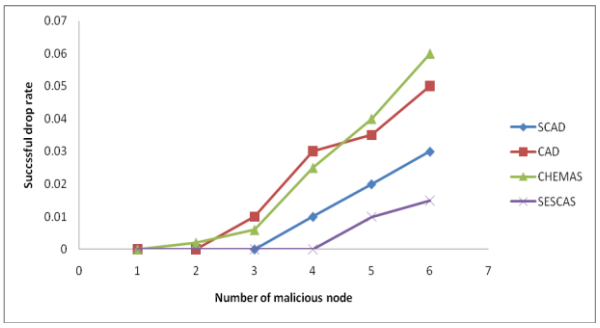

Figure.2. Number of malicious node vs successful drop rate

Figure.2. shows that relationship between malicious node and successful drop rate. Compared to SCAD, CAD and CHEMAS, the successful drop rate in SESCAS decreases. Both rejection rate and packet delivery ratio are measured by varying the malicious node and packet drop rate. In CHEMAS the successful drop rate is higher compared to CAD. The reason is that an acknowledgement packet makes less number of hops and thus each intermediate node receives less number of acknowledgement packets compared to that of CAD. In other words, multiple malicious checkpoint nodes can cooperate with each other and drop data packets without the knowledge of the user. Due to the victorious rejection rate, the packet transport ratio decreases. Compared to SCAD and CAD, the successful drop rate is more in CHEMAS. Note that the SESCAS shows zero successful drop rates while the SCAD shows 10% packet drop rate. In the figure.2, SESCAS show higher packet delivery ratio because the collision of multiple vicious nodes which is selected as a breakpoint or tagged node does not affect the SESCAS scheme. The SESCAS scheme offers packet retransmission feature in case, the data packet is lost (or) corrupted, hence this scheme provides the best performance (about 96% or more) in comparison to other schemes. The fig.3 shows that the SESCAS packet transport ratio increases 97% by zero successful drop rate.

Fig.3. shows that relationship between malicious node and packet delivery ratio. Compared to CHEMAS, SCAD and CHEMAS, packet delivery ratio in SESCAS increases. Both rejection rate and packet delivery ratio are examined by varying the malicious node and packet rejection rate. The packet delivery ratio is indeed a useful parameter to judge the efficient packet transmission when either of these schemes is employed in the communication channel. This parameter indicates the "extent to which the good and genuine (or) message rich packets is delivered to the destination node over the presence of cluster nodes (either genuine (or) malicious nodes). In other words, the ability of the scheme to scan message/content rich nodes and reject/suppress the malicious nodes is of greater concern. Hence, from figure. 3, the SESCA scheme wins the competition as it shows zero successful packet drop rates despite the presence of malicious nodes. Therefore, it is concluded from figure.3, that the SESCA scheme is a robust (zero successful packet drop) and dynamic (scans) one in comparison to other schemes.

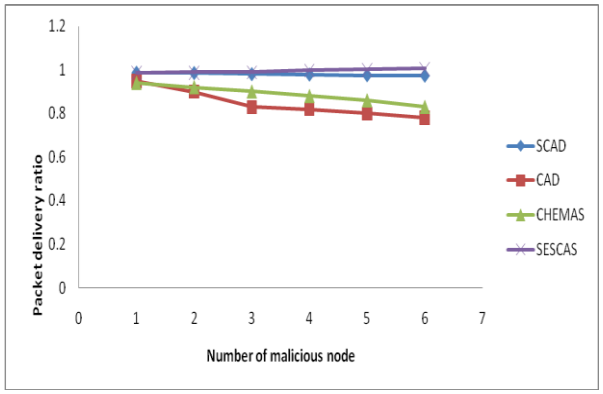

Figure.3. Number of Malicious node vs Packet delivery ratio

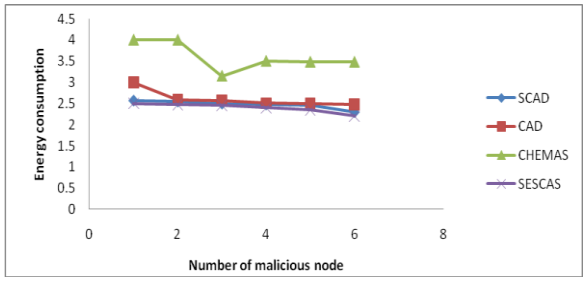

Figure.4. Number of malicious node Vs. Energy Consumption

Figure.4. shows that the relationship between malicious node and energy consumption. Compared to CHEMAS, SCAD and CAD energy consumption in SESCAS decreases. SESCAS represent minimal energy consumption when compared to that of SCAD and CAD due to the fact that low number of acknowledgement packets is generated (hence, duplicate detection of malicious packets is prevented) in the forwarding path. CHEMAS consumes more energy because packet drop is more compared to SCAD. The energy consumption in SESCAS is 15% less than the SCAD and CAD. In SCAD, the successful drop rate is more that shown in Fig.2. Due to this retransmission of packet occur. The retransmission leads to more energy consumption compared to SESCAS.

In SCAD, the energy consumption is 20% because of more packet drop in figure.4. In SESCAS the energy consumption decreases by 5%.

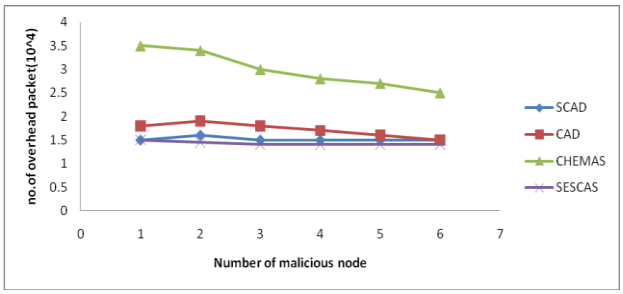

Figure.5. Number of Malicious node vs No. of overhead packet (10^4)

Figure.5 shows that relationship between malicious node and overhead packet. Compared to CHEMAS, SCAD and CAD, overhead packet decreases. The CHEMAS takes more time to transmit the data to the neighbouring node in the network. In the SESCAS, the data transmission rate is high due to Alarm packet. The delay in the transmission is also reduced. The transmission rate is very slow in CHEMAS and CAD. Compared to CHEMAS and CAD, the SCAD show higher transmission rate due to acknowledgement sent to the source. The detection of forward misbehaviour is better in SCAD compare to CHEMAS and CAD. In SESCAS, the time taken for packet transmission is less than SCAD. Due to the timer in the network, the node detects the malicious node and send acknowledgement to the source in the specified time.

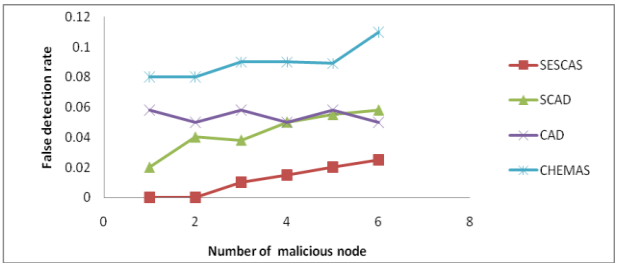

Figure.6. Number of malicious node vs false detection rate

Figure.6. depicts the relationship between malicious node and false detection rate. Compared to CHEMAS, SCAD and CAD, SESCAS scheme has a lower false detection rate. The SESCAS scheme dominates all other schemes when it comes to lower false detection rate. The reason is that the acknowledgement packets generated due to malicious node are suppressed, and therefore the energy consumption is considerably reduced. From the statistics shown above, the response delivered by SESCAS scheme is almost linear in comparison to other schemes. This indicates that the stable and smooth operation is attained with minimized false packet detection rate when SESCAS scheme is incorporated in communication channel.

These deviations arising between SESCAS and other schemes is the result of the fact that the other schemes unfortunately counts all the packet lost due to the poor channel quality, hence they exhibit greater probability of false detection rate. Also, it is strongly observed from the Figure. 6, that even for the presence of small number of malicious nodes, the other schemes miserably introduces larger number of false data packets in comparison to that of SESCAS scheme. Hence, it is evident that the SESCAS scheme provides better implementation when considerable packet detection is of greater concern.

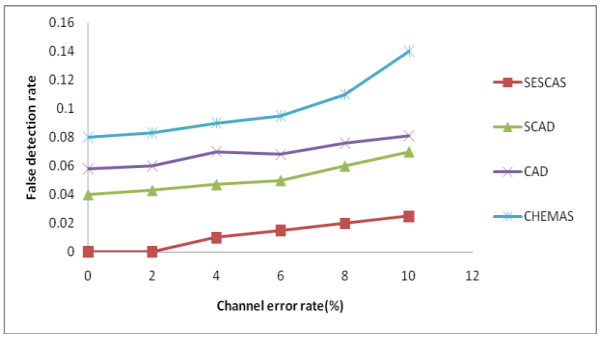

Figure.7. Channel error rate(%) vs False detection rate

Figure.7. shows that relationship between channel error rate and false detection rate. Compared to CHEMAS, SCAD and CAD, false detection rate decreases. The false recognition rate occurs due to the poor channel quality. The channel quality makes very harder to recognize the furtherance misbehaviour of vicious node. In SESCAS, the fake recognition rate is minimized because the number of acknowledgement packets generated by a single break point/debug node is reduced.

The channel quality is also better in SESCAS. Also, note that the SESCAS's fake recognition rate is smaller than that of the SCAD. Since, the SCAD miscounts the entire packets that are lost due to the poor channel quality: it presents higher degree of fake recognition rate. Multiple tagged nodes generates acknowledgement packet and each intercessor node frequently forwards them to the source in the CHEMAS. Hence, more acknowledgement packet can be lost due to the bad channel quality, and therefore resulting in higher fake recognition rate. In contrast to SESCAS, CAD with higher detection threshold value (i.e., 0.15) shows the highest fake recognition rate, because more intercessor nodes unfortunately accept a packet loss as a forward misbehaviour. Thus in SESCAS, the false detection rate is 0.11 than CAD and SCAD.

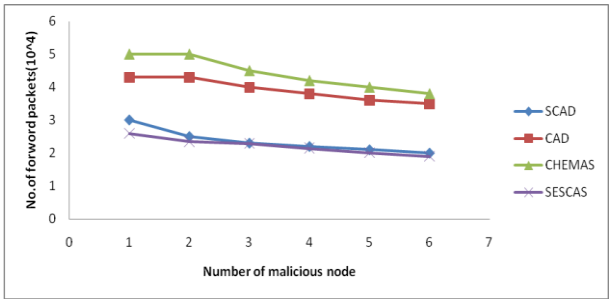

Figure.8. Number of malicious node vs number of forward packets

Figure.8. shows that relationship between malicious node and forward packets. Compared to CHEMAS, SCAD and CAD, forward packets decreases. The CHEMAS takes more time to transmit the user data to the neighbouring node in the network. The transmission rate is very slow in CHEMAS and CAD compared to CHEMAS and CAD, the SCAD show higher transmission rate due to acknowledgement sent to the source. The detection of forward misbehaviour is better in SCAD compare to CHEMAS and CAD. In the SESCAS the data transmission rate is high due to alarm packet. The delay in the transmission is also reduced. In SESCAS, the time taken for packet transmission is less than SCAD. Due to the timer in the network, the node detects the vicious node and send handshake signal to the source in the specified time. In SESCAS, the successful drop rate in Figure.1, reduces due to the acknowledgement sent to the source node and selectively forward the packet to the sink.

V. CONCLUSION

This paper proposes/introduces an atmosphere to circumvent the forwarding misbehaviour cluster, known as SESCAS. This system makes use of checkpoint node(s) approach facilitated by time-out and retransmission request features and formation of cluster indeed ensures that the false detection rate, energy consumption and frequent drop rates are minimized. In contrast to CHEMAS, CAD and SCAD schemes, SESCAS delivers optimum and acceptable (>95%) PDR using low energy/power for its operation. A simple abstract model of the SESCAS and its quantitative result in terms of fake recognition rate are also illustrated. Hence, to realize the full potential of the approach, the design parameters and possible extensions of the SESCAS are discussed. The simulation and quantitative result signifies that the proposed counter measure is a feasible implementation in WSNs.

REFERENCES

1. Wood, A.D. and Stankovic, J.A., Denial of service in sensor networks, computer, 35(10), pp.54-62, 2002.
2. Yu, Bo, and Bin Xiao, Detecting selective forwarding attacks in wireless sensor networks, Proceedings 20th IEEE international parallel & distributed processing symposium, PP 1-8, 2006.
3. Xiao, Bin, Bo Yu, and Chuanshan Gao, CHEMAS: Identify suspect nodes in selective forwarding attacks, Journal of Parallel and Distributed Computing, vol. 67, no. 11, pp. 1218–1230, 2007.
4. Shila, D.M., Cheng, Y. and Anjali, T., Mitigating selective forwarding attacks with a channel-aware approach in WMNs, IEEE transactions on wireless communications, vol. 9, no. 5, pp. 1661–1675, 2010.
5. Liu, Qiang, Jianping Yin, Victor CM Leung, and Zhiping Cai, FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs, IEEE Transactions on Wireless Communications vol. 12, no. 10, pp. 5124–5137, 2013.
6. Pu, Cong, Tejaswi Gade, Sunho Lim, Manki Min, and Wei Wang, Lightweight forwarding protocols in energy harvesting wireless sensor networks, In 2014 IEEE Military Communications Conference, pp. 1053-1059, 2014.
7. Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, Directed diffusion: A scalable and robust communication paradigm for sensor networks, Proceedings of the 9th annual international conference on Mobile computing and networking, pp 56-67, 2000.
8. Brad Karp and H. T. Kung, GPSR: Greedy Perimeter Stateless Routing for Wireless Networks, Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 243–254, 2000.
9. W. Stallings, Cryptography and Network Security—Principles and Practices, 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.
10. Sergio. Marti, T. J. Giuli, Kevin Lai, and Mary Baker, Mitigating routing misbehavior in mobile ad hoc networks, Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265, 2000.
11. Kukreja, Deepika, Sanjay Kumar Dhurandher and B. V. R. Reddy, Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack., Journal of Ambient Intelligence and Humanized Computing vol. 9, no.4, pp 941-956, 2018.
12. Ashokkumar S.R, MohanBabu G & Anupallavi S Multimed Tools Appl (2019). https://doi.org/10.1007/s11042-019-7359-0
13. Pu, Cong, Sunho Lim, Byungkwan Jung, and Jinseok Chae, EYES: Mitigating forwarding misbehavior in energy harvesting motivated networks. Computer Communications, 124, pp 17-30, 2018.
14. Ding, Derui, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275, pp 1674-1683, 2018.
15. Rai, Sandesh, Kalpana Sharma and Dependra Dhakal, A Survey on Detection and Mitigation of Distributed Denial-of-Service Attack in Named Data Networking, Advances in Communication, Cloud, and Big Data. Springer, Singapore, pp163-17, 2019.
16. Khari, Manju. "Wireless Sensor Networks: A Technical Survey." In Handbook of Research on Network Forensics and Analysis Techniques, pp. 1-18. IGI Global, 2018.
17. Modieginyane KM, Letswamotse BB, Malekian R, Abu-Mahfouz AM. Software defined wireless sensor networks application opportunities for efficient network management: A survey. Computers & Electrical Engineering, 66:274-87, 2018.
18. Zhang, Yushu, Yong Xiang, Leo Yu Zhang, Yue Rong, and Song Guo, Secure Wireless Communications Based on Compressive Sensing: A Survey, IEEE Communications Surveys & Tutorials (2018).
19. Yaseen, Q., Albalas, F., Jararwah, Y., & Al-Ayyoub, M.,Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks. Transactions on Emerging Telecommunications Technologies, 29(4), e3183, 2018.
20. Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S.H. and Gope, P., Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools and Applications, 77(14), pp.18295-18325, 2018.
21. Pu, Cong, and Sunho Lim, A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation, IEEE Systems Journal, 12(1), pp.834-842, 2018.
22. Thirukkumaran.R and Muthukannan.P (2016) "Security Issues in Wireless Sensor Networks on an Internet of Things (IoT) Platform", International Journal of Control Theory and Applications, Vol 9, Issue 35 pp 287-293.

AUTHORS PROFILE

Premkumar. M received B.E. degree on Electronics and Communication Engineering from Sri Subramanya College of Engineering and Technology, Palani, India in 2009. He acquired his Master's degree from the Karpagam College of Engineering, Coimbatore, India in 2012. At present, he is working in SSM Institute of Engineering and Technology, Dindigul as Assistant Professor. His research focus includes wireless channel security, authentication in ad hoc and sensor networks, and security in peer to peer systems.

Sundararajan. TVP received BE degree in Electronics and Communication from Kongu Engineering College, Bharathiar University, Coimbatore, Tamil Nadu (1993). He received his ME Degree in Applied Electronics from GCT, Bharathiar University, Coimbatore, Tamil Nadu (1999). He received his Ph.D degree from Anna University, Chennai (2013) for his work in Mobile Adhoc Network Security. At present, He is the Professor in Electronics and Communication Department, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamil Nadu. He has 20 Years of Teaching Experience in various colleges. His research interest includes cognitive

radio, ad-hoc networks, and radio resource management..

Bhuvaneswari. A received B.E. degree on Electronics and Communication Engineering from SSM Institute of Engineering and Technology, Dindigul, India in 2019. Her research focus includes wireless Sensor Networks and Network security.

Bhuvaneshwari. M received B.E. degree on Electronics and Communication Engineering from SSM Institute of Engineering and Technology, Dindigul, India in 2019. Her research focus includes wireless Sensor Networks and Network security.

Deepika. S received B.E. degree on Electronics and Communication Engineering from SSM Institute of Engineering and Technology, Dindigul, India in 2019. Her research focus includes wireless Sensor Networks and Network security.