ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume: 02 Issue: 05, May 2017, pp. 14 – 21

Flow Based Mitigation Model for Sinkhole Attack in Wireless Sensor Networks using Time-Variant Snapshot

Kannan Devibala
Assistant Professor, Department of Computer Science, Ayya Nadar Janakiammal College, Tamilnadu, India
Email: sreebalahoney@gmail.com

Dr. Saminathan Balamurali
Professor, Department of Computer Applications, Kalasalingam University, Krishnankoil, Tamilnadu, India
Email: sbmurali@rediffmail.com

Dr. Ayyanar Ayyasamy
Assistant Professor, Department of Computer Science and Engineering, Annamalai University, India
Email: samy7771@yahoo.co.in

Dr. Maruthavanan Archana
Assistant Professor, Department of Computer Science and Engineering, Annamalai University, India
Email: archana.aucse@gmail.com

Abstract: *Wireless Sensor Network (WSN) becomes popular at all levels due to the technology growth with equal frequency of risk towards various attacks. In this paper, proposes a novel Flow Based mitigation model to detect and mitigate Sinkhole attacks with the support of time variant snapshots (FBSD). The base station monitors the flow and at each time frame it computes the traffic transition pattern which shows the list of sensor node the packet has travelled. From the traffic pattern the presence of sinkhole is identified using snapshot of the network which is taken at different time frames. The base station maintains the location details of all the nodes in the network and assumes that the nodes are equipped with similar transmission range and capacities. The geographic and physical features of the node have been used to mitigate the sinkhole attacks*.

Keyword: *Sinkhole attack; Wireless sensor network; Time-variant snapshot; Traffic pattern.*

1. INTRODUCTION

Wireless Sensor Network (WSN) is a high frequent term pronounced by researchers during last decade due to the restrictions like limited energy and deployment nature induces the researchers to think more about WSN [1]. The loosely couple nature of WSN increases the feasibility of different attacks to be performed by adversaries. One among the possible attack is sinkhole attack which makes the overall traffic to be passing through a particular node [2, 3].

The sinkhole attack is one an adversary advertises its neighbors as the only neighbor which has shortest path [4] to reach the base station. While receiving this information what the neighbors will conclude is the adversary is located at most closure neighbor. Here after the neighbor nodes are forwards the packet through the sink which can perform any kind of attack in the network. The adversary can read packets which are coming from compromised nodes and perform modification, selective forwarding, and selective dropping attacks. So, that there is a higher requirement of protocols to detect mitigation of Sybil attacks [5, 6].

In WSNs the intermediate nodes participate in forwarding data packets to reach the destination. Once a group of node compromised with the adversary then the packets are passing through the same path to reach the destination [7]. The higher configured adversary has more power to generate Sybil attack and could participate in large number of transmission and routing processes. So, the traffic pattern and flow information's could be used to detect the Sybil attacks [8]. Flow based methodologies has been discussed in many papers in the literature but has not been utilized properly to detect and mitigate the Sybil attacks.

The presence of multiple adversaries makes the

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume: 02 Issue: 05, May 2017, pp. 14 – 21

traffic pattern to be changed at regular interval. The adversary can generate attack up to the time according to the energy constraint and will go to hell after that. So that the traffic patter will get change at each time frame [9, 10]. This feature could be used to find out the Sybil attack and adversaries.

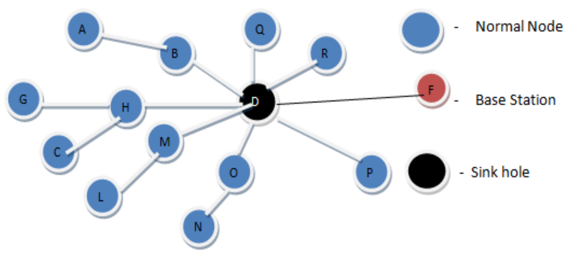

Figure 1 Network topology

The network snapshot is the most important metric which provides network topology information as shown in Figure 1. The topology of the network will get change at each time frame like entry of new nodes and death of few nodes [11]. The network snapshot taken at each time frame can be used to identify the presence of adversary. All this forced us to propose a novel flow based mitigation model for Sybil attack detection and used all the above discussed metrics of wireless sensor network to find out the Sybil attack and save network from mitigation.

The rest of the paper is organized as follows: Section 2 discussed about the related work. The challenges of the proposed work is discussed in Section 3 and briefly defined about the proposed model Flow based Mitigation Model in Section 4. Based on the work the achieved results are discussed in Section 5 and finally concluded the work in Section 6.

2. RELATED WORKS

Salehi et al., [12] have proposed a Sybil attack detection scheme which initially uses the consistency of data to find the group of suspected nodes. Then, the intruder is recognized efficiently in the group by checking the network flow information. This algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.

Chen et al., [13] have proposed a novel algorithm for detecting sinkhole attacks for large-scale WSNs formulate the detection problem as a change-point detection problem. Specifically, monitored the CPU usage of each sensor node and analyze the consistency of the CPU usage. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes. Rassam et al. [14], where the vulnerabilities of Mintroute protocol to sinkhole attacks are discussed and the existing manual rules used for detection are investigated using different architecture.

Devibala et al., [15], has proposed promiscuous mode method to detect and isolate the malicious node during wormhole attack by using ad-hoc on demand distance vector routing protocol with unidirectional antenna. The nodes which are not participating in multi-path routing generate an alarm message during delay and then detect and isolate the malicious node from network. Jin Qi et al., [16] have realizes a mechanism to launch sinkhole attack at WSNs and then present some mechanisms to detect and defense this type of attack. Finally, perform some experiments to verify our methods.

Otero and Hernández [17], have address a particular attack to the location and neighbor discovery protocols, carried out by two colluding nodes that set a wormhole to try to deceive an isolated remote WSN node into believing that it is a neighbor of a set of local nodes. To counteract such threat, present a framework generically called Detection of Wormhole Attacks using Range-Free method (DWARF) under which derive two specific wormhole detection schemes, the first approach, DWARFLoc, performs jointly the detection and localization procedures employing range-free techniques, while the other, DWARFTest, uses a range-free method to check the validity of the estimated position of a node once the location discovery protocol is finished.

Sheela et al., [18] have proposed a scheme to defend against sinkhole attacks using mobile agents. Mobile agent is a program segment which is self controlling. They navigate from node to node not only transmitting data but also doing computation. They are an effective paradigm for distributed applications, and especially attractive in a dynamic network environment. Ayyasamy [19] has discussed a routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sinkhole attack [20, 21]. The significant feature of the proposed mechanism is that it does not need any encryption or decryption mechanism to detect the sinkhole attack [22, 23]]. There are many works that have been carried out in the past by various researchers in the area of sinkhole attacks over wireless networks for providing effective security to networking systems [24-29].

3. PROBLEM STATEMENT

Most of the sinkhole detection mechanism uses various metrics which are computed based on traffic flow, geographic information and so on. Still there are problems with the earlier approaches as follows:

Network Overhead: some of the approaches use control messages to collect the neighbor information which increases the overhead of additional packets

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume: 02 Issue: 05, May 2017, pp. 14 – 21

transmitted and indirectly increases the traffic and latency in the network.

Throughput: The overhead generated by the earlier approaches due to network overhead reduces the packet delivery ratio and network throughput.

Energy Overhead: The transmission of control messages consumes some energy of all the nodes participate in flooding control messages which reduces the residual energy of all the nodes.

Lifetime: The energy overhead generated by flooding control messages and other protocol support packets reduces the life time of the node as well as whole network. Also if there is a centralized sinkhole detection mechanism it affects the energy and lifetime of a particular node or else if it is distributed one then it affects many number of nodes.

4. FLOW BASED MITIGATION MODEL

The proposed sinkhole detection mechanism has four different phases namely: Traffic Log Generation which generates the log about a particular traffic, traffic transition pattern –identifies the traffic pattern which has set of node names to represent the transition path, Time-Variant Snapshot which generates the topology snapshot of the network and finally Sinkhole Detection- which detect the sink node using the results of previous stages.

4.1 Traffic Log Generation

We assume that each node forwards the packet towards destination through some of its neighbors and appends the address of its own at the transition field of the packek.

TABLE I TRANSITION PATH

Source address	Destination address		Traversal path	Time
A	B	D	F	13:21:58
G	H	D	F	13:21:59
C	H	D	F	13:20:18
L	M	D	F	13:20:17
N	O	D	F	13:20:16

TABLE II TRAFFIC LOG GENERATION USING PACKET FRAME STRUCTURE

Seq. No.	PTYPE	Data Field	Source Address	Transition Address 1:2:3:4	Destination Address

The base station extracts the transition field and computes set of nodes present in the transition path logs (Table 1) to the data base (Algorithm 1). In Table 2, each node which forwards the packet adds its own address at the transition address field before forwarding the packet to the destination.

Algorithm 1: Traffic Log Generation

Step1: Start
Step2: Initialize traffic log TrLog. // TrLog-Traffic Log
Step3: receive packet P.
Step4: If packet Type == Data then
Extract the following fields.
Source Address SA = P (Source Address).
Destination Address DA = P (Dest. Address)
Time Received Tr = compute current Time.
Transition address TA = P (Transition Address).
TrLog = $(\sum TrLog) + (SA, DA, Tr, TA)$
End
Step5: Goto step3.
Step6: Stop

4.2 Traffic Pattern Generation

The traffic transition pattern (Algorithm 2) is computed using the log produced by the base station. The traffic log is cleaned before it used to detect the sinkhole, to overcome the unnecessary memory overhead generated by storing the entire traffic log for prolong period of time. Only a few numbers of traffic pattern will be maintained and at each time frame a new instance of traffic pattern will be feed into the traffic log table so that the last three time frame log only maintained at the traffic log. So that the log file contains the information about packets which are received at few previous time frames. The packets received at very old time will get deleted.

Algorithm 2: Traffic Pattern Generation

Step1: start
Step2: read traffic log table TrLog.
Step3: read traffic transition pattern table Tp.
Step4: for each log from TrLog
$TrLog_i$ = read log from TrLog.
//Extract Source Address SA,
//Transition path Trp,
//Destination Address DA, Time T_i from $TrLog_i$
Compute traffic transition path Tp_i = {Source Address, Destination Address Transition Path}.
$Tp_i = \sum Tp + (Tpi + Ti)$
End
Step5: for each log from TrLog
If $TrLog_i$ (T_i) < Time Frame end
Delete T_i from Log table.
TrLog =ϕ(TrLog, T_i).
End
Step6: stop.

4.3 Traffic Log Generation

Unlike other geostatic methods the propose method collects one time snapshot at the earlier time to get to know the topology information. From the topology information it generates the snapshot and updates the route table and node table (Algorithm 3). The route table contains information about set of nodes and routes to reach other nodes whereas the node table has information about the neighbors of the node. At later stage the base station generates the snapshot at regular time interval to detect the presence of sinkhole. Using the traffic pattern which is computed earlier, it finds out set of nodes which it feels guilty about working condition.

From the traffic pattern generated it verifies the presence of each node. If it does not find any node then it sends life cycle message to the guilty node and waits for the reply. Upon receiving the message the node which has not participate in any of the transmission in particular time window will reply with the message which contains information about the residual energy and neighbors. The control message will be passed to the guilty node only through the longest path which is not present in the traffic pattern. This assures delivery of life cycle message at the guilty node and it sends the reply through the path of request. This procedure reduces the overhead generated by flooding control message throughout the network to collect neighbor information's.

Algorithm 3: Time variant Snapshot

Start
Init Guilty set Gs, Timer T.
Read Traffic Pattern Table TP, Route table Rt, Node Table N, Snapshot S.
For each node N_i from N
For each traffic pattern Tp_i from Tp
Transition path
Trp = $\Delta \times (TPi, Tp(Traversl\ Path))$
If Trp $\ni Ni$ then
Else
Add to Gs = $\sum N + Ni$
End
End
End.
For each N_i from Gs
Compute Longest Path LP = $Max(\frac{RTi}{RT})$
Construct Life Cycle Message LCM
LCM = {Seq. No., Destination Address, Traversal Path - LP}.
Forward packet LCM
Start Timer T.
Receive LCM Reply from GS_i
If LCM Reply Received then
Update Neighbor table $\forall(Ni)$ = N + N_i.
Update Route Table $\forall(RTi)$ = Rt + Rt_i.
Update Snapshot S.
Else
End
End

4.4 Sinkhole Detection

The sinkhole detection procedure is executed at regular interval to find out the presence of sinkhole in the network. From that entries of generated traffic log as shown in Table 3. It computes the common node present in number of transition pattern. we call this set of node as guilty nodes Gs, for each from this set we compute the available routes using transition table based on computed routes and route from Traffic pattern (Trp), we analyze that whether the route present in the pattern is shorter or not. If the route is longer then we conclude that there is sinkhole and another control message will be sent to all the nodes to avoid sink hole from packet transmission as shown in Algorithm 4.

TABLE III GENERATED TRAFFIC LOG

Source Address	Destination Address	Traversal Path	Time
A	F	AB**D**F	13:21:58
G	F	GH**D**F	13:21:59
C	F	CH**D**F	13:20:18
L	F	LM**D**F	13:20:17
N	F	NO**D**F	13:20:16

Algorithm 4: Sinkhole Detection

step1: start
step2: read Traffic Pattern Table Tp, read Snapshot S.
step3: initialize guilty set Gs.
step4: compute common node from Tp.
AS-Adversary Set = N_i(N) $\ni \forall(TPi)$
step5: for each Tp from Tp
if $Tp_i \ni$ ASi then
Ap= compute available path from Route table Rt and snapshot S.
validate the distance of route used and routes from Ap.
if found guilty then
create alert message AM={seq. No, Source Addr, Destination Addr, Sinkhole Addr}
send AM through different path .
end.
end
end
step6: stop

5. RESULTS AND DISCUSSION

The proposed flow based sinkhole detection approach has been implemented in Network Simulator-2 (NS-2). We have designed network topology with different scenarios with different number of nodes. The proposed methodology has been evaluated with different density networks with multiple sinkhole

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume: 02 Issue: 05, May 2017, pp. 14 – 21

nodes. The following Table 4 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language and it uses Object Oriented Tool Command Language (OOTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

TABLE IV THE PARAMETERS USED IN OUR SIMULATION

Parameters	Value
Version	NS-allinone 2.28
Protocols	FBSD
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP, CBR
Packet size	512 bytes

TABLE V COMPARISON RESULTS FOR THROUGHPUT AND PDF

S. No.	No. of Nodes	Protocols	Detection Rate		Throughput	PDF
			False +ve	False -ve		
1.	71	Leader Based	4.5	3.0	85.0	80.90
2.		G-Hazard	3.5	2.5	92.0	86.70
3.		FBSD	0.9	0.8	97.8	93.50

5.1 Overhead

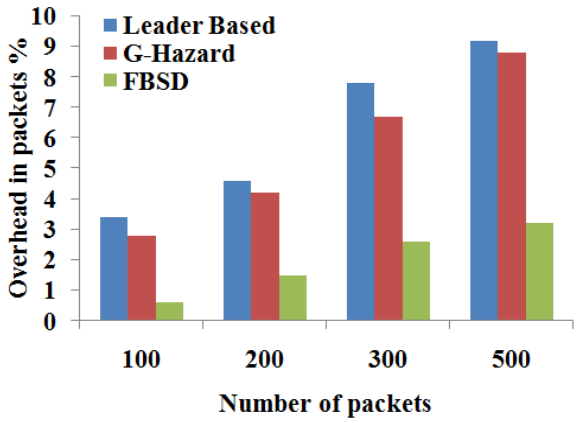

Figure 2 Overhead generated by sinkhole detection compared with existing methods

The overhead generated by sinkhole detection process has been shown in Figure 2. It shows that the proposed approach has produced less overhead than other methods while performing sinkhole detection process.

5.2 Throughput Performance

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps). Average throughput can be calculated by dividing the total number of packets received by the total end to end delay.

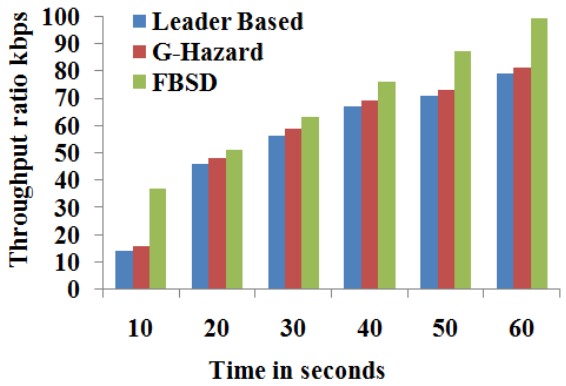

Figure 3 Throughput ratio of different methods

In Figure 3 shows the overall throughput ratio of different methods and it is clear that the proposed FBSD method has achieved higher throughput than other methods.

5.3 Packet Delivery Fraction:

The packet delivery fraction defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery fraction is computed as follows:

PDF = (No. of packets Received/No. of Packets Sent)*100.

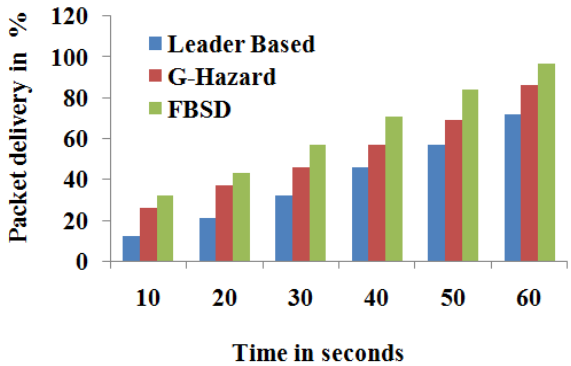

Figure 4 Packet delivery fraction compared with existing methods

In Figure 4 shows the performance of packet delivery fraction of different algorithms and it shows that the proposed FBSD method has higher packet delivery fraction than other methods.

5.4 Average End-to-End delay

Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, and delay at the MAC due to retransmission, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a MANET from source to destination.

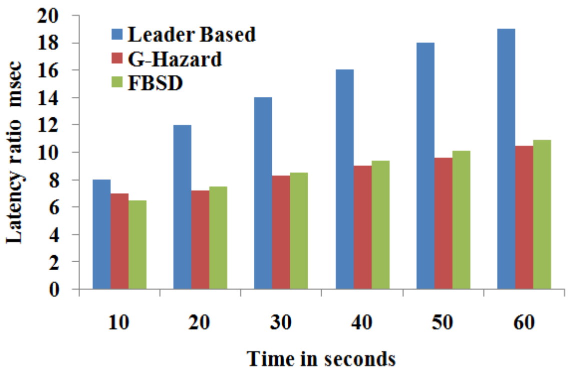

Figure 5 End-to-end delay compared with existing methods

In Figure 5 shows the latency ratio of different methods and it shows clearly that the proposed method has lower latency ratio than others.

6. CONCLUSION

The proposed FBSD method monitors the traffic flow and extract the features of traffic and produces logs into the data set. Then traffic transition patter is generated to compute the traversal path of the packet. At the third stage a time variant snapshot of the network is generated using the traffic transition pattern generated, finally the mitigation detection is performed using the transition patter and snapshot of the network. The aim of the FBSD was reducing various control overheads which are generated due to various reasons and particularly by flooding the control messages. The proposed method highly reduces the overhead generated by flooding control messages in the network and increases the performance of the network.

REFERENCES

[1] Harold Robinson, Y, Golden Julie E, Balaji S, Ayyasamy A., “Energy Aware Clustering Scheme in Wireless Sensor Network Using Neuro-Fuzzy Approach” , *Wireless Personal Communications*, pp. 1-19, 2016.

[2] Ayyasamy and K. Venkatachalapathy, “Increased throughput for load based channel aware routing in MANETs with reusable path”, *International journal of computer applications (IJCA)*, Vol. 40, No. 2, pp. 20-23, February 2012.

[3] I. Shin, N. Pham, and H. Choo, “Virtual convex polyg on based hole boundary detection and time delay based hole detour scheme in WSNs”, *in: Human Interface and the Management of Information. Designing Information Environments*, pp. 619–627, 2009.

[4] K. Devibala, S. Balamurali, A. Ayyasamy and M. Archana, (2016), “Neighbor constraint traffic centric distributed sinkhole detection and mitigation approach for quality of service improvement in wireless sensor networks”, *In: Proceedings of the international conference Industry Interactive Innovations in Science, Engineering and Technology (I3SET 2016)*, Lect. Notes in Networks, Syst., Bhattacharyya, ed al. (Eds), Vol. 11, 2017.

[5] C. Baquero P. Almeida, R. Menezes, and P. Jesus, “Extrema propagation: Fast distributed estimation of sums and network sizes”, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 4, pp. 668-675, 2012.

[6] R. Villalpando, C. Vargas, and D. Munoz, “Network coding for detection and defense of sinkholes in wireless reconfigurable networks”, *in: Proceedings of International Conference on Systems and Networks Communications*, pp. 286–291, 2008.

[7] S. Tamilselvan, K. Venkatachalapathy and A. Ayyasamy, “An efficient energy conservation using diffusion update algorithm in wireless sensor network”, *International journal of control theory and applications*, Vol. 9, No. 2, pp. 521-529, May 2016.

[8] K. Devibala, S. BalaMurali, and S. Venkateselu, “Decentralized detection and mitigation of sinkhole attacks in wireless sensor networks based on network density estimation technique”, *International Journal of Control Theory and Applications*, Vol. 9, No. 1, 2016.

[9] B. Choi, E. Cho, J. Kim, C. Hong, and J. Kim, “A sinkhole attack detection mechanism for LQI based mesh routing in WSN” *in: Proceedings of International Conference on Information Networking*, pp. 1–5, 2009.

[10] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, “Intrusion detection of sinkhole attacks in wireless sensor networks”, *In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*, pp. 150-161. Springer Berlin Heidelberg., 2007.

[11] I. Krontiris, T. Giannetsos, and T. Dimitriou, “Launching a sinkhole attack in wireless sensor networks; the intruder side”, *in: Proceedings of IEEE International Conference on Wireless and Mobile Computing*, pp. 526–531, 2008

[12] Salehi, S.A., Razzaque, M.A., Naraei, P. and Farrokhtala, A., “Detection of sinkhole attack in wireless sensor networks”, *IEEE International Conference on Space Science and Communication (IconSpace)*, pp: 361-365, 2013.

[13] Chen, C., Song, M. and Hsieh, G., “Intrusion detection of sinkhole attacks in large-scale wireless sensor networks”, *Wireless Communications, Networking and Information Security (WCNIS)*, pp. 711-716, 2010.

[14] Rassam, M.A., Zainal, A., Maarof, M.A. and Al-Shaboti, M., “A sinkhole attack detection scheme in Mintroute wireless Sensor Networks”, *IEEE International Symposium on Telecommunication Technologies (ISTT)*, pp. 71-75, 2012.

[15] K. Devibala, S. BalaMurali, and S. Venkateselu, “Sheltered Confidentiality on Spots for Mobile Based Social Application”, *in: Proceedings of the National Conference On Recent Trends in Computer Science, Applications & Engineering*, pp. 227-234, 2016.

[16] Qi, Jin, Tang Hong, Kuang Xiaohui, and Liu Qiang., “Detection and defence of Sinkhole attack in Wireless Sensor Network”, *IEEE 4th International Conference on Communication Technology (ICCT)*, Vol. 9, pp. 809-813, 2012.

[17] Otero, M. G., and Hernández, A. P., “Secure neighbor discovery in wireless sensor networks using range-free

localization techniques”, *International journal of distributed sensor networks,* Vol. 2012, pp. 1-12, 2012.

[18] D. Sheela, C. Naveen Kumar, and G. Mahadevan, “A non cryptographic method of sinkhole attack detection in wireless sensor networks”, *IEEE International conference on recent trends in information technology,* pp. 527-532, 2011.

[19] A. Ayyasamy, “Development of Channel based Routing Mobile Ad hoc Network” Doctor of philosophy Thesis, Annamalai University, Annamalainager, Tamilnadu, India. pp. 1-135, 2015.

[20] A. Ayyasamy and K. Venkatachalapathy, “Context aware adaptive service based dynamic channel allocation approach for providing an optimal QoS over MANET”, *International journal of engineering and technology (IJET),* vol. 6, no. 3, pp. 1465-1479, 2014.

[21] A. Ayyasamy and K. Venkatachalapathy, “Context aware adaptive fuzzy based Quality of service over MANETs*”, International review on computers and software (IRECOS),* vol. 9, no. 7, pp. 1220-1226, 2014.

[22] Selvakumar Kamalanathan, SaiRamesh Lakshmanan, Kannan Arputharaj, “Intelligent Energy Aware Multiple Quality of Service restraints based Secured Optimal Routing Protocol with Dynamic Mobility Estimation for Wireless Sensor Networks”, *Transylvanian Review,* Vol. 24, No. 5, 2016.

[23] Harold Robinson, Y, Rajaram, M., Golden Julie, E. and Balaji, S., “Detection of Black Holes in MANET Using Collaborative Watchdog with Fuzzy Logic”, *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering,* Vol. 10, No. 3, pp. 575 – 581, 2016.

[24] A. Ayyasamy and K. Venkatachalapathy, “Performance evaluation of load based channel aware routing in MANETs with reusable path”, *International journal of engineering and advanced technology (IJEAT),* Vol. 3, No. 1, pp. 183-186, November 2013.

[25] M Selvi, R Logambigai, S Ganapathy, L Sai Ramesh, H Khanna Nehemiah, Kannan Arputharaj, “Fuzzy Temporal Approach for Energy Efficient Routing in WSN*”, In Proceedings of the International Conference on Informatics and Analytics, ACM , 2016. DOI:10.1145/2980258.2982109.*

[26] Balaji S, Harold Robinson Y, Rajaram M, “SCSBE: Secured Cluster and Sleep Based Energy-Efficient Sensory Data Collection with Mobile Sinks”, *Circuits and Systems,* vol. 7, issue 8, pp. 1992-2001, 2016.

[27] A. Ayyasamy and K. Venkatachalapathy, “An improved load balancing adaptive QoS buffer scheduler (I-LABS) for steaming services over MANET”, *International journal of computer science and engineering technology (IJCSET),* vol. 5, no. 5, pp. 612-620, 2014.

[28] M. Thanga Aruna, E. Golden Julie, and Y. Harold Robinson, “A Survey on Techniques for Selection of Forwarding Node in Wireless Sensor Networks”, International Journal of Advances in Computer and Electronics Engineering, Vol. 02 , No. 04, pp. 24-29, April 2017.

[29] Pratham Harshit Rajmahanty, and S. Ganapathy, “Role of Decision Trees in Intrusion Detection Systems: A Survey”, International Journal of Advances in Computer and Electronics Engineering, Vol. 02, No. 04, pp. 09-13, April 2017.

Authors Biography

K. Devibala is an Assistant Professor, Department of Computer Science, Ayya Nadar Janaki Ammal College, Sivakasi. She received her M.Sc in Computer Science and Information Technology from the Madurai Kamaraj University of India, in 2008. She has the credit of publishing nearly 5 research articles in the referred and peer reviewed international journals/ conferences and presented nearly 2 papers in the national conferences. Her research interest is in Wireless Sensor Networks, QoS and routing protocol, computer network as well as network security.

Dr. S. Balamurali is a Professor of Statistics at Kalasalingam University. He received his MSc and Ph.D degrees from Bharathiar University, India. He has the credit of publishing nearly 52 research articles in the referred and peer reviewed international journals/ conferences and presented nearly 15 papers in the national conferences. His research interests include Statistical process control acceptance sampling and analysis of means, Wireless Sensor Networks, QoS and routing protocol as well as network security.

Dr. A. Ayyasamy is B.E. and M.E. in Computer Science and Engineering from Annamalai University, Chidambaram, Tamilnadu, India in the year 2006 and 2008 respectively. He is working as Assistant Professor in Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University from 2007 where he obtained his Doctorate in 2015. He has the credit of publishing nearly 34 research articles in the referred and peer reviewed international journals/conferences and presented nearly 8 papers in the national conferences. His areas of interest are mobile ad-hoc network, wireless network, streaming media architectures, QoS and routing protocol, computer engineering as well as network security. He is also serving as Editor-in-chief of International Journal of Networking (BioInfo publications). He is also serving as an editorial board member for various international journals, and reviewer in IEEE, Springer, Ad Hoc and Sensor Wireless Networks (AHSWN) etc. He also accepted an invitation to be a Technical review committee member for many international conferences (India, USA, London, Malaysia...). He is a professional member of ACM journals, International Association of Engineering, and senior member in Universal Association of Computer and Electronics Engineers. He received Young Faculty award from Center for Advanced Research and Design in 2015.

Dr. M. Archana is an Assistant Professor in Information Technology, Department of Computer Science and Engineering at Annamalai University since 2008. She received her B.E degree in Information Technology with gold medal and stood one among the gold medalist of Annamalai University in 2007. She received her M.E (Distinction) degree in Computer Science and Engineering from Annamalai University in the year 2011. She was completed her Ph.D in 2016. Her areas of interest are image and video processing, broadcast tennis video, pattern classification and wireless network. She has the credit of publishing nearly 09 research articles in the referred and peer reviewed international journals and presented nearly 2 papers in the national conferences. She is a member of International Association of Engineering.