International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

A Trust Model for Security Against Black Hole Attack in Hierarchical Cluster Based Wireless Sensor Network

Ganesh R. Pathak, M.S. Godwin Premi, Suhas H. Patil

Abstract : Wireless Sensor Network (WSN) is widely gaining fame since it has theoretically unavoidable unlimited applications. Security stays a significant challenge for WSN because for a few feeble substances like open remote medium, dynamic topology, absence of centralized infrastructure and intermittent network connectivity. Dark gap assault is a sort of Denial of Service (DoS) attack, which influences reliability of a system by diverting and dropping genuine packets in the system. Black hole attack ends up being progressively extraordinary when number of threatening nodes participate to show Black hole attack in the framework, which is named as a helpful black hole attack. In this paper, we showed an Enhanced Detection and Prevention Mechanism for Black hole Attack (EDPMBA) Trust Model to save the assurance from single and helpful black hole attack. EDPMBA additionally shows better execution as far delay and packet conveyance proportion.

***Keywords*: Wireless Sensor Network, Trust, Black Hole Attack, Security**

I. INTRODUCTION

Wireless Sensor Network (WSN) is a versatile system contained huge number of little minimal effort devices known as sensor nodes and few general-purpose processing devices referred as base stations [1, 3, 5].A sensor node is able to ob- serve parameters like temperature, sound, vibration, pressure, motion or pollutants of a certain area. The measured values are then forwarded to a base station, which is in-charge of further processing [6]. Security is a major concern in WSN because of several weak entities like open wireless medium, dynamic topology, absence of centralized infrastructure and intermittent connectivity [10]. Black hole attack is one of the critical Denial of Service (DoS) attack where the malicious node attracts packets and subsequently drops these packets. The situation becomes more serious when number of malicious nodes gets involved in introducing black hole attack, which is referred as cooperative black hole attack. We are motivated by the need to preserve security of WSN against such single and cooperative black hole attacks and presented an Enhanced Detection and Prevention Mechanism for Black gap Attack (EDPMBA) Trust Model. Major contributions of our research work are as follows:

1. To build up a trust model to ensure the WSN against single and cooperative black hole attack.
2. Simulation results show that EDPMBA is proficient regarding delay and packet delivery ratio of the of the system considering black hole attack.

Remaining paper is organized as follows: Section II presents the literature survey. Section III describes the system model. Section IV presents the proposed Enhanced Detection and Prevention Mechanism for Black hole Attack Trust Model. Section V briefs about the performance evaluation followed by conclusion in Section VI.

II. LITERATURE SURVEY

In previous research work, various solutions are introduced to secure WSN against black hole attack. To encounter a single or a team of black hole attacks, Karakehayov [18] came across a novel approach for developing a routing algorithm Receive Watch Redirect (REWARD) for wireless sensor network. As soon as the misbehavior nodes detected, REWARD creates a distributed database to store the malicious nodes and their respective location. Tiwari et al. [7] introduced the local information based system in which even though sensor nodes

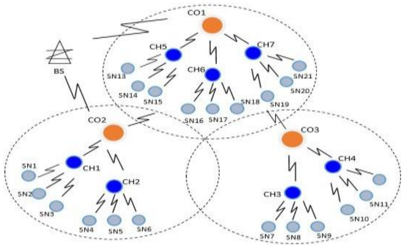

Fig. 1. Hierarchical Cluster Topology in Wireless Sensor Network

Revised Manuscript Received on November 22, 2019

Ganesh R. Pathak, Associate Professor in the Department of Information Technology of Sinhgad College of Engineering, Pune (Maharashtra), India.

Dr. M.S. Godwin Premi, Professor in School of Electrical and Electronics Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.

Dr. Suhas H. Patil, Professor Department of Computer Engineering, Bharati Vidyapeeth University, Pune (Maharashtra), India.

Retrieval Number: D9219118419/2019©BEIESP
DOI:10.35940/ijrte.D9219.118419

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

do not aware of the global view, still an attack can be detected based on local information. To achieve this, they proposed an algorithm, which follows specification-based concept where the nodes behavior is taken into consideration and based on that action will be decided. Tree topology is used in the sensor network in which entire network is divided into clusters wherein each cluster is treated as a leaf of a tree and cluster head is identified as a parent of the cluster. Malicious node detection mechanism in wireless sensor network can be evaluated depending upon the individual node's trustworthiness [9, 11, 15, 17]. Generally, each sensor node is responsible for trust evaluation based on monitoring its neighbor node's behavior. The corresponding node decreases the trust factor for its neighbor node if it is acting maliciously [2,4]. Mathur et al.[8] have introduced similar approach by building a trust model against black hole. Few security solutions concern about mobile environment, network's scalability, its adaptability and node's energy [12,13,14]. Our work is motivated by the secu- rity solution presented by Wazid et al. [16]. In [16], authors proposed a solution to remove a black hole attacker node from the network. The solution is limited to detection of malicious nodes inside the cluster. If the node joins another cluster, it may introduce infected packets. In the proposed solution, once the malicious node get detected it cannot introduce black hole attack by joining any other cluster and thus is more secure than [16].

III.SYSTEM MODEL

System model briefs about the network model of the presented work and describes about how single and black hole attack works in this network model.

A. Network Model

In this work, we considered cluster-based network for WSN. Figure 1 shows cluster based WSN comprising of all possible nodes. The network contains four types of nodes. Large number sensor nodes (SN) sense the environmental data and forwards to cluster head (CH) node. In each cluster, there exists one or more CHs, which collect raw data from respective SNs, process the data and send the resultant values to Coordinator Nodes (CO). CO is responsible for handling the robustness of the network and handles the issues such as node failure or link failure. Finally, CO sends data to Base station (BS).

B. Single and Cooperative Black Hole Attack

Figure 2 illustrates how single black hole attack actually acts inside the system. Sensor hubs SN1, SN2, SN3 sense the occasions and report it to its Cluster Head 1 (CH1). Additionally, SN4, SN5, SN6 report to Cluster Head 2 (CH2). Afterward, CH1 and CH2 total the gathered information and forward it to Cluster Coordinator CO. On the off chance that CH2 turns into a black hole node, at that point it ingests whole traffic towards it and drops every one of the bundles as opposed to transmitting it further to CO.

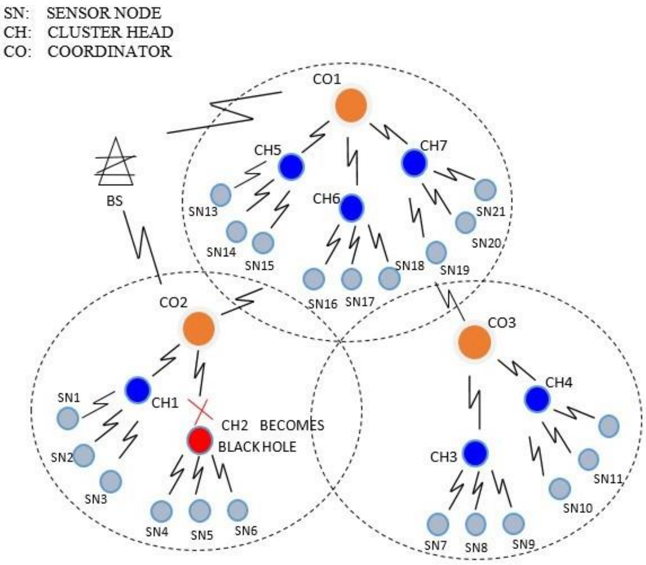

Fig. 2. Single Black Hole Attack

Cluster Head CH2 and sensor hub SN11 are black hole nodes and work together to assume responsibility for whole system. At the point when a sensor hub SN2 from group 1 and SN9 from Cluster 2 send a course solicitation to the destination, black hole nodes CH2 and SN18 react promptly with the phony course answer parcel imagining as they are the quick neighbors to the goal thus contain the most brief way towards it. After receiving a route reply, SN2 and SN9 dismiss all authentic answer packets originating from neighboring nodes and they start sending information packets to black hole nodes accepting that Packets will arrive at the destination. Later on, CH2 may transmit those packets to SN18 and SN18 drops every one of the packets and vice versa.

TABLE
I LIST OF SYMBOLS

Symbol	Description
t lmt	Time for which a node works as coordinator
battery pow	Battery power of coordinator
trust threshold	Trust threshold value
energy threshold	Energy threshold
loop list	List created for a node if get trapped in looping
wait tm	Waiting threshold time for coordi- nator in receive mode
w tm	Waiting threshold time for interme- diate node in receive mode
IDj	ID of Black Hole node
ARRV RESP DATA	Response packet and data packet both arrive
NOT ARRV RESP DATA	Response packet and data packet both not arrived
ARRV RESP NOT ARRV DATA	Response packet arrived but data packet not arrived

Algorithm 1: Algorithm for Enhanced Detection and Prevention Mechanism for Black hole Attack (EDPMBA) Trust Model

1. Initiate node disclosure process.
2. Evaluate Trust Model:

Trust Model:

2a. /A node accepting hi packet from neighboring node,

(i) Assign an underlying trust esteem (trust) to neighboring node and keep up a table for trust estimations of all nodes.

(ii) If a neighbor node is available on top of it listthen
new trust = down * trust;/down = const worth ought to be less
else
new trust = up * trust ;/up =const worth ought to be more prominent than down

(iii) Update trust an incentive for neighboring node 2b. /Generate a rundown of neighboring nodes

3. //Route Discovery Procedure

3a. / A node accepting course demand parcel from neighboring nodes,

(i) Obtain the Delivery Ratio (DR I) and trust I esteems for neighboring nodes

(ii) If (DR I < trust I) at that point

new trust = down * trust I + DR I ;/down = const esteem expel a neighboring node from a rundown
else
new trust = up * trust I + DR i ;/up =const esteem

(iii) Update trust an incentive for neighboring node

3b. /Periodically, Obtain the trust and vitality esteems for neighboring node

In the event that (trust i < trust limit && expended energy > vitality limit) at that point by means of guide signal.

Discard a packet

4. Maintaining a cluster of all sensor nodes as
$CH = \{SN_1, SN_2, SN_3, SN_4, ..., SN_n\}$

5. Allocate the node identification N_{ID} to all nodes as
$N_{ID} = \{N_{ID1}, N_{ID2}, N_{ID3}, ..., N_{IDn}\}$

6. Selection of a coordinator (SN_i) from the set CH as per condition for some time, all the residual nodes are in the supervision of this node 6a. // criteria fairness

Node act as a coordinator up-to certain time limit <= tm lmt

6b. // criteria efficiency

Node act as a coordinator if it has battery power >= battery pow

7. Coordinator is maintaining a table for identification (ID) of all nodes

8. S_i periodically checks the ID of each node from the set C = $\{ SN_1, SN_2, SN_3, SN_4, \;, SN_{(i-1)} , SN_{(i-1)} ..... SN_n \}$

9. //Black opening assault discovery and aversion in the event that (ARRV RESP DATA) at that point no interruption risk

else if (NOT ARRV RESP DATA) on the off chance that (w tm >= hold up tm) at that point nodes disappointment
else
w tm++;
else on the off chance that (ARRV RESP NOT ARRV DATA) at that point
on the off chance that (w tm >= hold up tm) at that point
the hub can be a vindictive node (dark opening) recognizes its ID
(IDj)
else
w tm++;

10. Remove that hub from the cluster CHN =
{ SN1, SN2, SN3, SN4, ..., SN(j−1), SN(j+1), , SNn }

11. Inform its past hubs through reference point signal for the node with which now they need to impart.

12. Reformation of group with node set as CHN =

{ SN1, SN2, SN3, SN4, ..., SN(j−1), SN(j+1), , SNn }

13. Continue the trust assessment and recognition process.

IV.AN ENHANCED DETECTION AND PREVENTION

MECHANISM FOR BLACK-HOLE ATTACK (EDPMBA) TRUST MODEL

EDPMBA Trust Model has two phases: nodes discovery and trust initialization followed by node selection and revocation. After the discussion of these two phases we explore the routing procedure. Algorithm for the proposed trust model is presented in Algorithm 1 which uses list of symbols listed in Table I.

A. *Node discovery and Trust Initialization*

During the lifetime of the system, after a particular interim, node revelation procedure is done by sending hello packets. A sensor node communicates hello packets to find its neighbors. On gathering of hello bundles, neighboring hubs would choose reliability of a node from which they are accepting hello packets. Assume node I finds its neighbors by sending hello bundles. On gathering of hello packets, a node j would choose a reliability of node I. An underlying trust metric for a neighbor node I is introduced by ascertaining a proportion of number of hello packets node j has gotten from node I to the quantity of hello parcels sent. In the following case, node j will look into the nearness of node I on the up and up list, on the off chance that node I is available on the up and up list, at that point decline its trust an incentive by some steady factor signified as "down", and estimation of down is set to "0.3".

In the event that node

I is absent insider savvy list, at that point increment its trust an incentive by some steady factor say "up" and its worth is set to "0.5". Include the neighbor into neighboring rundown and thus update the comparing trust an incentive for node I and store it into trust table.

On the off chance that a hub is available on the up and up list, at that point
new trust = down * trust ;/down = const esteem else
new trust = up * trust ;/up =const worth Update trust an incentive for neighboring hubs

B. Nodes selection and Revocation

In this stage, a dependable node will be chosen for correspondence and deceitful node will be boycotted. While neighboring node j accepting a course demand packets from node state I, its dependability will be assessed. To assess this, right off the bat, a conveyance proportion for a neighbor node is determined as the proportion of number of information packets got from node I to the quantity of information bundles sent. Simultaneously, an old trust worth is gotten for node I. In the event that the Delivery proportion for node I is discovered not exactly old trust estimation of node I at that point decline the trust an incentive for node I by some steady factor indicated as "down", and estimation of down is set to "0.3" and don't acknowledge the course demand from node I, intend to state, expel a node from a rundown. On the off chance that trust worth is discovered more prominent than its conveyance proportion, at that point increment its trust an incentive by some steady factor say "up" and its worth is set to "0.5". At last update the relating trust an incentive for node I.

i. A node getting course demand packets from neighboring node, Obtain the Delivery Ratio (DR I) and trust I esteems for neighboring nodes. in the event that (DR I ¡ trust I) at that point

new trust = down * trust I + DR I ; else
new trust = up * trust I + DR I ;

Also, get the vitality esteem for a neighbor node and confirm how much vitality it has expended till it procedures further. Confirmation ought to be accomplished for both trust and vitality esteems.

ii. If trust and vitality esteems are come to past foreordained trust limit and vitality edge, at that point dispose of a packets.

B. Routing Procedure

EDPMBA runs an intermittent pattern scheme. The length of that period decides how much of the time steering data is traded and refreshed. After a precise interval, node discovery process is initiated which creates the neighboring nodes list. Cluster is formed among those set of neighbors and CH and CO are elected to play a proficient role in the overall communication and packet transmission process. Before a node starts with actual data packet forwarding process, it has to establish a path towards destination node to which it has to communicate or send a data packet. So, it initiates a route discovery process by sending route request packets. Trust metric plays a major role to set up a secure path.

C. Performance Evaluation

EDPMBA is implemented using Network Simulator (NS2). Simulation parameters utilized in the experimentation are recorded in Table II. Every one of the node has a similar power level and the equivalent maximal transmission scope of 100 m. A Constant Bit Rate (CBR) traffic is created with User Datagram Protocol (UDP) association. CBR packet size is picked to be 512 bytes in length. Duration of the scenarios is 200 seconds and the sense time for node began at time equivalents to 35.0 seconds and proceeds until the finish of the simulation.

TABLE II SIMULATION PARAMETERS

Parameters	**Values**
Simulation Area	1000 * 1000
No. of Nodes	30, 50, 75
Simulation time	200 Sec.
Transmission Range	100m
Energy model	100 J
Pause time	25 m/s

Performance of EDPMBA is compared with traditional detection and prevention mechanism for black hole attack (DPMBA) [10] . Figure 3 to Figure 5 shows comparative evaluation of EDPMBA and DPMBA in terms of average energy utilization, delay and packet delivery ratio (PDR) with and without black hole attack.

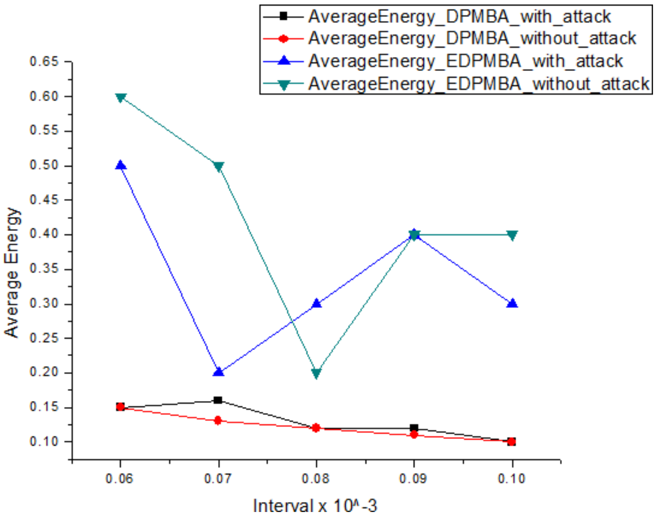

Fig. 3. Intervals Vs Average Energy with and without attack

In terms of PDR and end-to-end delay, proposed EDPMBA shows better results than DPMBA. As DPMBA makes use of waiting time mechanism which may cause more delay

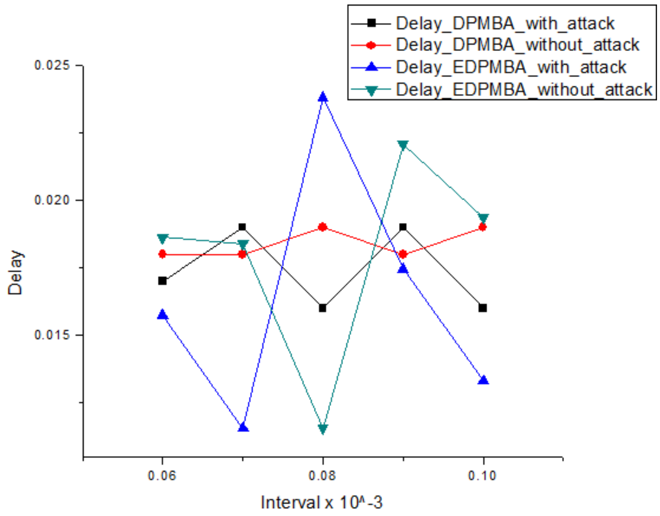

Fig. 4. Intervals Vs Delay with and without attack

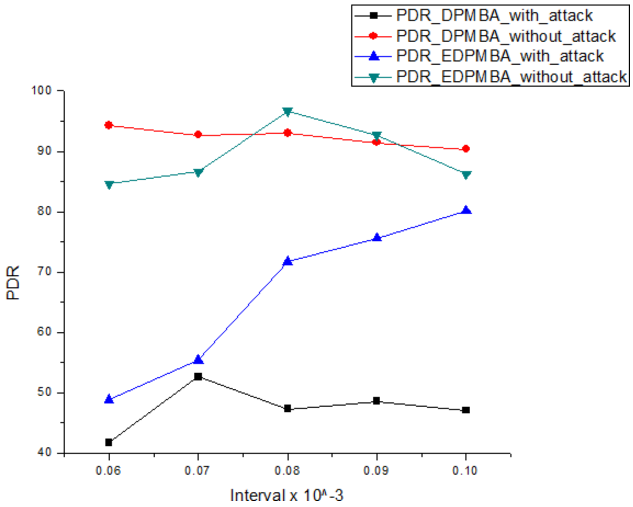

Fig. 5. Intervals Vs PDR with and without attack

and throughput in packet transmission whereas with trust model in proposed system reduce such delay by separating misbehaving nodes at earlier stage. In case of enegry requirement, EDPMBA gives better results in terms of PDR and end-to-end delay. Since, DPMBA makes use of waiting time mechanism, it causes more delay in packet trasfer and also reduces the PDR. The proposed EDPMBA overcomes this limitation by separating misbehaving nodes at earlier stage. Proposed mechanism requires a little bit more energy than DPMBA. But the energy loss is marginable with the advantages in terms of trustworthiness of neighbours.

V. CONCLUSION

Black hole attack is one of the Denial of Service attacks which acts alone or in cooperation to lure entire traffic towards it and prevent it further reaching to the base station by dropping all packets. The proposed trust model reports a successful and secure instrument for identification of single and cooperative black hole attack and gives a protected routing path from sensor node till base station. This method continues acting mischievously node from being a piece of a system correspondence process before real black hole identification system is started. Simulation results shows better per-formance of EDPMBA as far as delay and PDR which is the basic prerequisite in WSN. In future, the proposed trust model can be tried for portable WSN where sensor nodes can be versatile.

REFERENCES

1. Baadache, A., & Belmehdi, A. (2014). Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 73, 173–184. doi:10.1016/j.comnet.2014.07.016.
2. Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M (2012). Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent. International Conference on Artificial Intelligence and Embedded Systems.
3. Djahel, S., Nait-Abdesselam, F.,& Zhang, Z. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. IEEE Communications Surveys and Tutorials, 13(4), 658–672. doi:10.1109/SURV.2011.072210.00026.
4. M. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar and D. P. Singh (2013). Detection and prevention mechanism for blackhole attack in Wireless Sensor Network. Communications and Signal Processing (ICCSP), International Conference on, Melmaruvathur, pp. 576-581.
5. Pantazis, Nikolaos A., Stefanos A. Nikolidakis, and Dimitrios D. Vergados (2013). Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials 15. no. 2, pp. 551-591.
6. Hidoussi, F., Toral-Cruz, H., Boubiche, D. E., Lakhtaria, K., Mihovska, A., & Voznak, M. (2015). Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks. Wireless Personal Communications, 85(1), 207–224. doi:10.1007/s11277-015-2734-2.
7. Tiwari, M., Arya, K. V., Choudhari, R., and Choudhary, K. S. (2009). Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. In 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology (pp. 824-828). IEEE.
8. Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. Sensors (Switzerland), 16(1). doi:10.3390/s16010118.
9. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering, 40(2), 530–538. doi:10.1016/j.compeleceng.2013.06.001.
10. Petridou, S., Basagiannis, S., & Roumeliotis, M. (2013). Survivability analysis using probabilistic model checking: A study on wireless sensor networks. IEEE Systems Journal, 7(1), 4–12. doi:10.1109/JSYST.2012.2224612.
11. Poongodi, T., & Karthikeyan, M. (2016). Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks. Wireless Personal Communications. doi:10.1007/s11277-016- 3318-5.
12. Saravana Kumar, N. M., Deepa, S., Marimuthu, C. N., Eswari, T., & Lavanya, S. (2015). Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission. Wireless Personal Communications, 87(2), 431–442. doi:10.1007/s11277-015-3070-2.
13. Shu, T. S. T., Krunz, M., & Liu, S. L. S. (2010). Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. IEEE Transactions on Mobile Computing, 9(7), 941–954. doi:10.1109/TMC.2010.36.
14. Su, M.-Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), 107–117. doi:10.1016/j.comcom.2010.08.007.
15. Umang, S., Reddy, B. V. R., & Hoda, M. N. (2010). Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption. IET Communications, 4(17), 2084. doi:10.1049/iet-com.2009.0616.
16. Atul B.Kathole , Yogadhar Pande "Survey Of Topology Based Reactive Routing Protocols In VANET" International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 39 ISSN 2229-5518
17. Wazid, M., Katal, A., Singh Sachan, R., Goudar, R. H., & Singh, D.
18. P. (2013). Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network. International Conference on Communication and Signal Processing, ICCSP 2013 - Proceedings, 576–581. doi:10.1109/iccsp.2013.657712.

AUTHORS PROFILE

Ganesh R. Pathak received Bachelor of Engineering (B.E.-Computer) from Walchand Institute of Technology, Maharashtra, India and Master of Engineering (M.E. - CSEIT) from University of Pune, Maharashtra, India. He is currently working toward the PhD degree in Computer Science and Engineering at Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India. He is presently working as an Associate Professor in the Department of Information Technology of Sinhgad College of Engineering, Pune. His research interests include Computer Networks, Wireless Communication, Wireless Sensor Network, especially security in wireless sensor network..

Dr. M.S. Godwin Premi is presently working as a Professor in School of Electrical and Electronics Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India. She has a total teaching experience of 18 years. She has more than 50 research papers to her credit in reputed national and international journals and conferences. Presently 8 candidates are pursuing their Ph.D. under her guidance. Her research interests include sensor networks, image processing and cryptography.

Dr. Suhas H. Patil received Doctor of Philosophy (Ph.D.) Degree in Computer Science and Engineering from Bharati Vidyapeeth University, Pune. He is presently working as a Professor Department of Computer Engineering, Bharati Vidyapeeth University, Pune, India. He has a total teaching

Retrieval Number: D9219118419/2019©BEIESP
DOI:10.35940/ijrte.D9219.118419

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication