International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN

Ganesh R. Pathak
Associate Professor
Department of IT, SCOE, Pune

Suhas H. Patil
Professor and Head
Bharati Vidyapeeth University College of Engg,Pune

Jyoti S. Tryambake
PG Student
Department of IT, SCOE, Pune

ABSTRACT

In a Wireless Sensor Network (WSN), Security is a key challenge due to its dynamic topology, open wireless medium, lack of centralized infrastructure, intermittent connectivity, resource constrained sensor nodes. These weak entities make WSN easily compromised by an adversary to device abundant attacks resulting in disastrous consequences. Black Hole can be one of them wherein it exploits a trustworthiness of a network by promising routing of data packets to the destination knowing that it has a shortest path but in reality it drops all packets and consequently threatens reliability. In order to accomplish secure packet transmission, an efficient and trust based secure protocol is proposed to defend against single and cooperative Black Hole attack. A proposed protocol incorporates trust metric estimation to determine honesty of nodes during secure path formation. A proposed system builds a Hierarchical Cluster Topology and is experimentally evaluated to demonstrate its effectiveness in detecting and preventing efficiently the Black Hole attacks. Besides, comparison of proposed protocol with one of the existing approach [9] proves that proposed system is efficiently reduces possibility of misbehaving nodes being a part of network communication process and achieves better packet delivery ratio, throughput and less end-to-end delay. The Simulation results signify that the proposed protocol performs satisfactorily in secure routing and is robust against both single and cooperative Black Hole attacks in a dynamic environment.

Keywords

Wireless Sensor Network, Security, Black Hole attack, Hierarchical Cluster Topology.

1. INTRODUCTION

Wireless Sensor Network (WSN) finds its applications [1] in multiple areas like; homeland security, environment and monitoring purposes, military, agriculture and manufacturing tasks etc. where security is an important perspective [4] comes into picture. For an extensive wireless network, it is not viable to observe and protect each individual node from variety of attacks. To make entire network system unsteady attackers may perhaps launch different types of security threats mostly during routing phase. Attacks on routing ([2], [3]) can be done in two phases; first phase is attack on routing protocol by jamming the flooding of information to a node. For example, Hello flood attack, Acknowledgement spoofing etc. and another phase belongs to attack on packet delivery mechanism by creating a predefined path in order to direct traffic towards it. Black Hole attack [5] is one of the examples that falsely advertises a less enough distance route to the destination and forces entire traffic to go through Black Hole region.

Significant research effort has been spent on designing defense mechanisms for Black Hole attack studied in [16]; which are complex, energy inefficient and scarce to protect a network when multiple nodes act cooperatively to perform malicious activity and may have devastating impact on overall network. In this paper, an efficient and trust based secure routing protocol to discover and prevent Single and Cooperative Black Hole attack is presented. The approach is straightforward and trust based to determine honesty of nodes in order to accomplish secure packet transmission.

Main contribution of this work is divided into three phases. In first phase, simulations of solution proposed for Black Hole attack by Mohammad Wazid et al. [9] is implemented. Second phase enhances the algorithm to improve accuracy in preventing Black Hole attack. Proposed algorithm does not give any implementation details of existing algorithm but addresses several issues of [9] during performance. In third phase, a comparison of proposed mechanism with the existing solution [9] is performed in terms of performance parameters [17] such as Packet Delivery Ratio, Throughput, End-to-end Delay.

Rest of the paper is structured as follows: Section 2 briefly survey existing security solutions in WSN for Black Hole attack. Section 3 describes proposed security protocol for single and cooperative Black Hole attack in a dynamic WSN. In Section 4, performance of the proposed security solution is evaluated and presented in the form of graphs. Section 5 concludes the paper.

2. RELATED WORKS

To encounter a single as well as team of Black Hole attacks, Karakehayov Z. [6] has suggested a REWARD (Receive, Watch, Redirect) method with the help of two broadcast messages; MISS and SAMBA to identify Black Hole nodes. This method works well for different levels of security. Tiwari M. et al. [7] have introduced the concept of watchdogs to watch behavior of nodes that facilitates further to detect malicious nodes performing anonymous activity. D S. et al. [8] have proposed a novel approach to improve data delivery in the presence of a Black Hole attack that uses concept of multiple base stations deployed in WSN using mobile agent. The purpose of multiple base stations is to ensure high packet delivery in the presence of attack. Atakli I. M., Hu H. et al. [11] have developed a Weighted Trust Evaluation (WTE) mechanism for hierarchical sensor network architecture. This mechanism is applied to Cluster Head at every cycle to detect anonymous activity. Dr. Virmani D. et. al. [12] proposed an exponential trust based mechanism to detect malicious node. Trust factor drops exponentially with each consecutive packet dropped which helps in detecting the malicious node. Janani C et. al. [13] introduced TARF a robust trust aware routing framework for WSNs mainly protects a WSN against the replay attacks and also, proved to be powerful against strong attacks such as wormhole attacks and Sybil attacks. An innovative approach is proposed by Athmani S. et al. [10] based on periodic control message exchange mechanism between a sensor node and a base station. This mechanism requires a bit energy load due to packet exchange scheme.

Wazid M. et al. [9] considered a tree topology in WSN for their work and invented a detection and prevention mechanism for Black Hole attack. This tree topology consists of sensor nodes, router nodes and a coordinator node (CO). Coordinator node supervises all nodes in the network, carries out authentication phase and thus detects the intruder node if any in the network with the help of waiting time parameter. The mechanism [9] has come across several shortcomings such as this algorithm works for static sensor network and did not consider mobility of nodes. Indeed, a Black Hole node is removed from particular cluster but in future it may affect another cluster as a result, there are very less chances for WSN to become completely safe against Black Hole attack. Besides, this method is not suitable for cooperative Black Hole attack. This paper simulates proposed system that improves the existing solution [9] and makes it more efficient and accurate to prevent Black Hole attacks. At the end, a performance is measured both for proposed and existing system.

3. PROPOSED SECURITY SOLUTION

Basic idea is to develop robust and reliable solution to detect and prevent Black Hole attack in dynamic WSN with minimum energy consumption and less delay. The proposed solution builds hierarchical cluster topology and identifies single as well as cooperative Black Hole attack in a mobile environment. Most of the solutions discussed earlier identify malicious node only after an attack is taken place. To circumvent this situation, the existing system [9] is improved with introducing trust model to decide a trustworthiness of nodes going to participate in communication process. Proposed system tries to eliminate infected and misbehaving node from being a part of communication process. Initially, proposed security solution builds a Hierarchical Cluster Topology to achieve energy efficiency criterion ([14], [15], [16]). Soon after, a security protocol is applied to the network to identify any anonymous activity. Following section describes Cluster formation, Black Hole Attack Scenario and implementation of efficient and trust based secure protocol is elucidated thereafter.

3.1 Hierarchical Cluster Topology

Proposed system uses Hierarchical Cluster Topology consists of four levels in WSN comprising a Sensor Node (SN), Cluster Head (CH), Coordinator Node (CO), Base Station (BS) as shown in Figure 1.

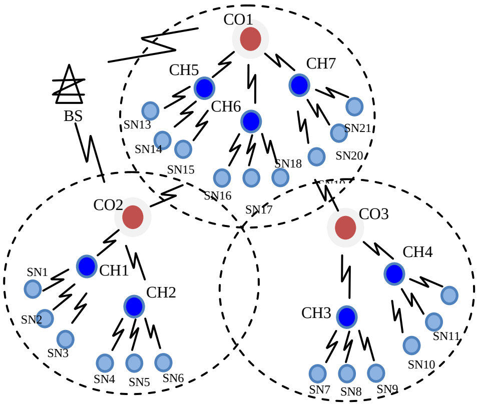


Figure 1. Hierarchical Cluster Topology

The whole network is divided into number of clusters and each cluster consists of one or more than one CH, a CO and that controls numerous SNs. The CHs of different clusters communicate with each other to switch over aggregated data. CHs forward aggregated data to the CO and finally to the Base-Station. Four different levels of WSNs are described as below:

Level-1: Sensor nodes sense the medium, gather raw data and forward it to the second level that is to CH.

Level-2: These are special-purpose sensor nodes called as Cluster Heads (CHs). In each cluster, there exists more than one cluster head, which collect raw data from several SNs from a cluster. Each CH of the network has unique ID. CHs come across several events using SNs of its own cluster and prepare final report using data aggregation techniques, and forwards collective data to the third level that is to CO.

Level-3: These are Coordinator nodes (CO) forward raw fused and aggregated data to next level Cluster or Base Station. CO in each cluster is elected by sensor nodes in that cluster. Election of a cluster coordinator requires two things to be considered.

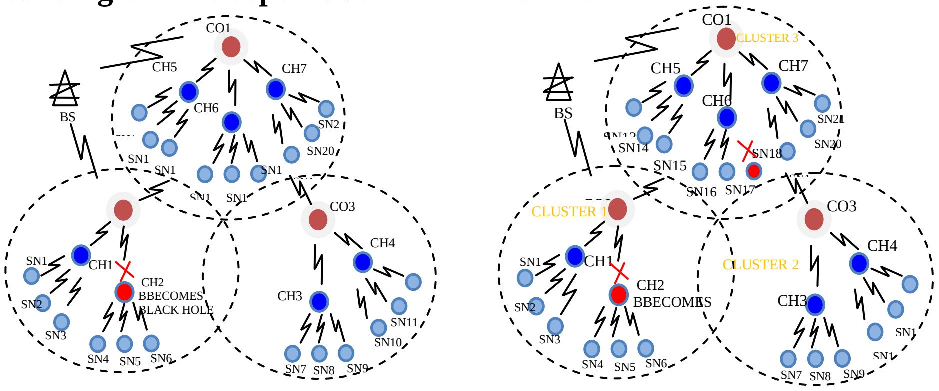
- Equality: Any node can turn into a CO that means the probability of every node being a cluster coordinator should be equal.

- Efficiency: *A* node from the cluster having high efficiency i.e. high battery backup can be periodically selected.

All sensor nodes are in the monitoring zone of coordinator node. CO is mainly responsible for authentication, checking for node failure and detection of Black Hole node if exists in the network.

Level-4: These are high-bandwidth sensing and communication nodes form fourth level of the network and are known as the Base-Station (BS).

3.2 Single and Cooperative Black Hole Attack



(a) Single Black Hole Attack **(b) Cooperative Black Hole Attack**

Figure 2. Black Hole Attack

Figure 2 (a) illustrates Single Black Hole attack in the network. Sensor nodes SN1, SN2, SN3 sense the events and report it to its Cluster Head 1 (CH1). Similarly, SN4, SN5, SN6 report to Cluster Head 2 (CH2). Later, CH1 and CH2 aggregate collected data and forward it to Cluster Coordinator CO. If CH2 becomes a Black Hole node then it absorbs entire traffic towards it and drops all packets instead of transmitting to CO.

In Figure 2 (b), CH2 and SN11 Black Hole nodes work together to take control over entire network. When a sensor node say SN2 from cluster 1 and SN9 from cluster 2 send a route request to the destination, Black Hole nodes CH2 and SN18 respond immediately with fake route reply packet pretending as they are immediate neighbors to the destination and so contain shortest path to towards it. After receiving a route reply SN2 and SN9 would reject all legitimate reply packets coming from neighboring nodes and they start sending data packets to Black Holes believing that packet will reach the destination. Later on, CH2 may transmit those packets to SN18 and SN18 will drop all packets and vice versa.

3.3 Black Hole Attack Detection and Prevention Using Proposed Trust Model

As discussed earlier, a Trust for a node corresponds to its prior performance in the form of its packet delivery and looking forward its presence into a

Looping. Looping is term where node transmits and receives same packets from neighboring nodes. Looping is evaluated because it highly affects data packet delivery, throughput, may cause more delay and mainly cause devastating impact on nodes energy.

3.3.1 Trust Model

Proposed Trust metric is an additional piece of action carried out in waiting_time based Black Hole attack detection mechanism [9]. As soon as a network is established and nodes initiate neighbor discovery procedure, a Trust for every node is evaluated before actual Black Hole attack detection process begins. A Trust Model is distributed in two phases; First phase is associated with Nodes Discovery and Trust Initialization and Secondly, Nodes Selection and Revocation are described further.

3.3.1.1 Nodes Discovery and Trust Initialization

After a specific interval nodes discovery process is carried out by sending hello packets. A node broadcasts hello packets to discover its neighbors. On reception of hello packets, neighboring nodes would decide trustworthiness of a node from which they are receiving hello packets. Suppose node i discovers its neighbors by sending hello packets. On reception of hello packet, a node j would decide a trustworthiness of node i depending upon its prior performance in the form of packet transmission. An initial trust metric for a neighbor node i is initialized by calculating its packet delivery ratio.

In next case, node j has to look up the presence of node i in the loop list, if node i is present in the loop_list then its trust value decreased by some constant factor denoted as “down”. If node i is not present in the loop_list, then increase its trust value by some constant factor say “up”. Add neighbor into neighboring list and consequently updates corresponding trust value for node i and store it into trust table.

```
If a node is present in the loop_list then
        new_trust_ = down * trust_ ;     // down = const value
Otherwise
        new_trust_ = up * trust_ ;      // up =const value
Update trust value for neighboring nodes
```

3.3.1.2 Nodes Selection and Revocation

In this phase a trustworthy node would be selected for communication and untrustworthy node will be blacklisted. By the time, neighboring node j receiving a route request packet from node say i, its trustworthiness would be evaluated. To estimate this, firstly, a packet delivery ratio of a neighbor node is calculated. At the same time, an old trust value is obtained for node i. If the Delivery_ratio for node i is found less than old trust value of node i then decrease the trust value for node i by some constant factor denoted as “down”, and do not accept route request from node i. If trust value is found greater than its delivery ratio then increase its trust value by some constant factor say “up”. Lastly update corresponding trust value for node i.

```
(i) A node receiving route request packet from neighboring nodes,
Obtain the Delivery_Ratio (DR_i) and trust_i values for neighboring nodes
If (DR_i < trust_i) then
        new_trust_ = down * trust_i + DR_i ;// down = const value
        remove a neighboring node from a list
Otherwise
        new_trust_ = up * trust_i + DR_i ;     // up =const value
Update trust value for neighboring nodes
```

In addition, obtain the energy value for a neighbor node and verify how much energy it has consumed till it process further. Verification should be done for both trust and energy values.

(ii) If trust and energy values are reached beyond predetermined trust_threshold and energy_threshold then discard a packet.

Proposed protocol runs a periodic service as similar to many routing protocols. After a precise interval, nodes discovery process initiated which creates neighboring nodes list. Nodes illustrate trust of their neighbors by examining their packet delivery ratio and occurrence into loop list. Initially, Trust metric is estimated in nodes discovery procedure that looks up for a node in Looping. If a corresponding node is under influence of looping, trust factor associated with it get decreased otherwise it may further be incremented. Similar case is evaluated under route request circumstance where Route request procedure determines energy consumption for requested node. In this case a trust value evaluation for a node is solely depends upon its delivery ratio. This trust metric reduces chances of a failure or infected node to become a part of a communication process in the network. And thus, node crossing trust threshold and consuming more energy would be kept aside from a path generating process and so, secure path can be formed to the destination node. Later on, Cluster Coordinator node takes a responsibility to identify a malicious and failure node inside the network with the help of waiting_time procedure [9].

4. SIMULATION

4.1 Simulation Environment

Proposed work is simulated using network simulator tool NS2. A network of square surface of 1000×1000m^2 is constructed for simulation purpose. Initially, proposed experimental model is built on 50 nodes distributed randomly and move arbitrarily on a simulation area. Later on, it is evaluated for rising number of nodes such as for 75,100 and 125. All nodes have same power level and same maximal transmission range of 100m. A CBR

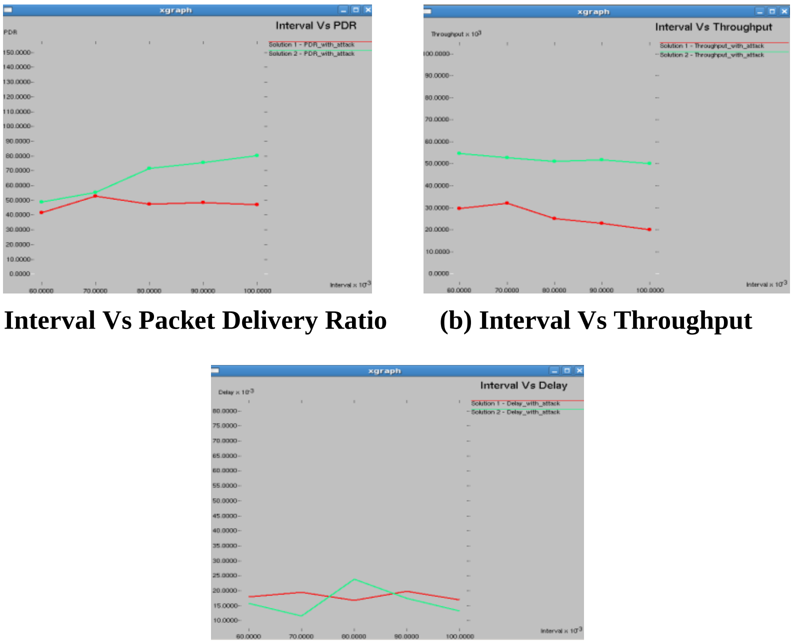
(Constant Bit Rate) application is attached that generates constant packets through UDP connection. CBR packet size is preferred to be 512 bytes long. A node initiates packet transmission from a random location and when destination is reached a transmission process repeats after 25m/s pause. Simulation takes place for 200 seconds. Simulation parameters are summarized below in Table 1.

Table 1. Simulation Parameters

Parameters	Values	Parameters	Values
Environment Area	1000 * 1000	Packet Size	512
Topology	Hierarchical Cluster	Energy model	100 J
No. of Nodes	50, 75, 100, 125	Pause time	25 m/s
Simulation time	200 Sec.	Traffic source	CBR
Transmission Range	100m	Channel Type	Wireless

4.2 Simulation Results

The performance of proposed protocol is analyzed against Black Hole attack in terms of amount of data packets delivered to the Base Station and delay caused during this transmission. For this purpose, two Black Holes are assumed randomly deployed in a network and act individually as well as cooperatively. With the presence of Black Holes, performance is measured in terms of Packet Delivery Ratio (PDR), Throughput, End-to-end Delay at several intervals for existing system [9] say Solution 1 and also for proposed system say Solution 2 shown in following graphs.



(a) Interval Vs Packet Delivery Ratio

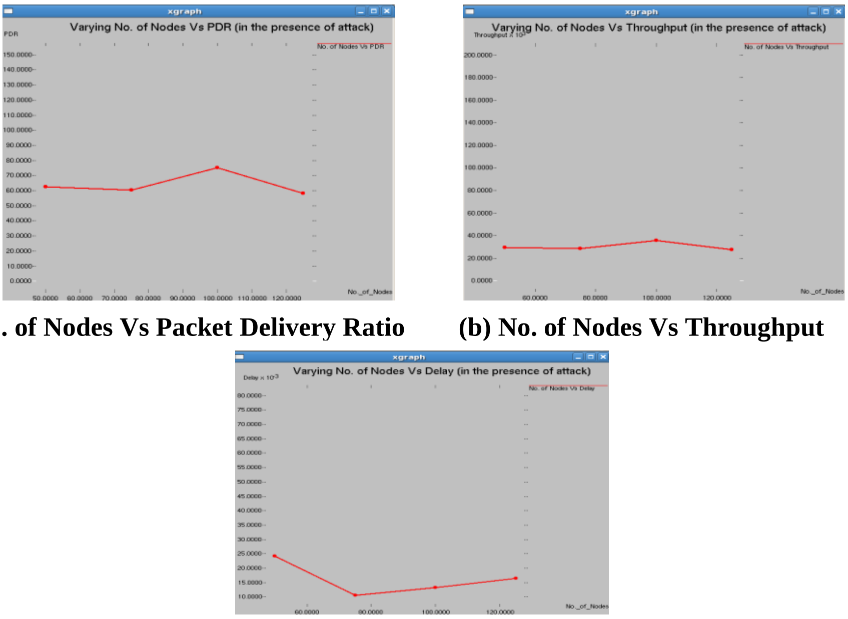
(b) Interval Vs Throughput

(c) Interval Vs End-to-end Delay

Figure 3. Comparison Graphs

Figure 3 shows comparison of solution proposed by [9] and proposed solution, by which several observations such as the Solution 1 [9] heavily suffers from Black Hole attack. Figure 3(a) depicts that Solution 2 raises PDR by 30 to 40% whereas in Figure 3 (b), Solution 2 achieves better throughput almost twice the throughput obtained in Solution 1. However Figure 3 (c) demonstrates impact of attack on end-to-end delay. Solution 2 accomplishes less end-to-end delay than Solution 1 since it takes less time to find a secure route by exempting misbehaving nodes at initial stage.

In Solution 1, a node responding to route request can be selected to form a secure path and further, a Coordinator node is responsible to detect any anonymous activity by waiting for incoming packets over a period of time. This procedure may introduce more delay and also affects throughput. Whereas, Solution 2 prefers a node with its trust assessment that presents its prior performance. If a node is observed performing well then that would be selected to form a secure path. Consequently, it can be stated that trust based solution mitigate significantly Black Hole attack. Evaluation of trustworthiness of nodes gives better results as compared to waiting_time based Black Hole attack detection procedure. Trust Metric estimation achieves improved Packet Delivery Ratio (PDR), Throughput and obtains less end-to-end delay. Proposed solution is additionally tested for increasing number of nodes to examine its scalability and adaptability for real-time scenarios. For this purpose, PDR, Throughput and Delay are investigated for varying number of nodes and with the presence of Black Hole attack. Following Figure 4 shows results of performance parameters for varying number of nodes.



(a) No. of Nodes Vs Packet Delivery Ratio **(b) No. of Nodes Vs Throughput**

(c) Number of Nodes Vs End-to-end Delay

Figure 4. Graphs for Varying Number of Nodes

Figure 4 (a), Figure 4 (b) and Figure 4 (c) signify that proposed solution works satisfactorily for increasing number of nodes. There is no significant difference achieved in PDR, Throughput and Delay for increasing number of nodes. It is observed that trust based solution detects Black Hole nodes despite rising number of nodes and proficiently scalable to real time environment. Most importantly, to optimize effective utilization of proposed system under real time scenarios and greater number of nodes additional resources need to be provided.

5. CONCLUSION

Introduction of proposed efficient and secure routing protocol to identify single and cooperative Black Hole attack chains in a self-motivated environment and thereby generates a secure routing path from source node to the destination node. Proposed protocol encloses a feasible trust based solution that examines trustworthiness of neighboring nodes. This approach keeps misbehaving nodes aside from being a part of a network communication process before actual Black Hole detection procedure is initiated. Proposed protocol has formed a Hierarchical Cluster Topology and simulated at several intervals. A proposed solution as well as solution proposed by [9] is simulated using Network Simulator Tool NS2 and performance is analyzed in terms of Packet Delivery Ratio, Throughput and End-to-end Delay. Simulation results depict that proposed system has been highly effective and adaptable under dynamic environment circumstances and accomplishes significant improvement than existing solution [9]. Additionally, a trust based solution is experimentally observed to be scalable to medium-scale test bed environment for different simulated conditions. A trust based system is packet traffic efficient and time efficient as it facilitates significant improvement in data delivery for dynamic topology with minimum delay.

REFERENCES

[1] Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E., *Wireless sensor networks: a survey*, Elsevier Science B.V., Computer Networks 38 (2002), 393–422, 2002.

[2] Goyal P., Parmar V., Rishi R., MANET: Vulnerabilities, Challenges, Attacks, Application, *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, January 2011.

[3] Razak S. A., Furnell S. M., Brooke P. J., *Attack against Mobile Ad Hoc Networks Routing Protocols*, University of Plymouth.

[4] T. Kavitha, D. Sridharan, Security Vulnerabilities in Wireless Sensor Networks: A Survey, *Journal of Information Assurance and Security*, Vol. 5, pp. 031-044, 2010.

[5] Sen J., Koilakonda S., Ukil A., *A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks*, Tata Consultancy Services Ltd.

[6] Karakehayov Z., *Using REWARD to detect team black-hole attacks in wireless sensor networks*, In ACM Workshop on Real-World Wireless Sensor Networks, 2005.

[7] Tiwari M., Arya K. V., Choudhari R., Choudhary K. S., Designing Intrusion Detection to Detect Black Hole and Selective Forwarding Attack in WSN based on local Information, *Fourth International Conference on Computer Sciences and Convergence Information Technology*, IEEE, 2009.

[8] Sheela.D, Srividhya.V.R, Begam A, Anjali and Chidanand G.M., Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent, *International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012)* , July 15-16, 2012.

[9] Wazid M., Katal A., Singh R., Sachan, Goudar R. H., Singh D. P., Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network, *International conference on Communication and Signal Processing*, IEEE, April 3-5, 2013.

[10] Athmani S., Boubiche D. E., Bilami A., Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs, *IEEE*, 2013.

[11] Atakli I. M., Hongbing H., Yu Chen, Wei-Shinn Ku, Zhou Su, *Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation*, SpringSim, 2008.

[12] Dr. Virmani D., Hermrajani M., Chandel S., *Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network*.

[13] Janani C., Chitra P., Trust Evaluation Based Security in Wireless Sensor Network, *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, Vol. 2 Issue 1, January 2013.

[14] Wei C., Yang J., Gao Y., Zhang Z., Cluster-based Routing Protocols in Wireless Sensor Networks: A Survey, *International Conference on Computer Science and Network Technology*, IEEE, 2011.

[15] Singh S., Singh M. P., Singh D. K., A Survey of Energy-Efficient Hierarchical Cluster-Based Routing in Wireless Sensor Networks, *International Journal of Advanced Networking and Applications*, Vol. 02, Issue 02, pp. 570-580, 2010.

[16] Tryambake J. S., Pathak G. R., Patil S. H., A Survey on Black Hole Attack Detection and Prevention Methods in MANET and WSN, *3rd International Conference on Recent Trends in Engineering and Technology (ICRTET'2014)*, Elsevier Publication, Vol. 1, 28-30 March, 2014.

[17] Ebenezar jebarani M.R. and Jayanthy T., An Analysis of Various Parameters in Wireless Sensor Networks Using Adaptive Fec Technique, *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, Vol.1, No.3, September 2010.

This paper may be cited as:

Pathak, G. R.., Patil, S. H., Tryambake, J. S., 2014. Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN. *International Journal of Computer Science and Business Informatics, Vol. 14, No. 2, pp. 93-103*.