International Conference on Academic Research in Engineering and Management
IETE, Lodhi Road, Delhi, India (ICAREM-17)
30th April 2017, www.conferenceworld.in ISBN: 978-93-86171-43-6

GENERATION MECHANISMS OF SINKHOLE ATTACK IN ROUTING PROTOCOLS OF WIRELESS SENSOR NETWORK

Amit kumar jangid[1], Dr. Nonita sharma[2], Ankur bohora[3]

[1,2,3]*Department of Computer Science & Engineering, National Institute of Technology Delhi, (India)*

ABSTRACT

The proposed research work is an attempt to demonstrate the intrusion detection system for sinkhole attack in wireless sensor network. First, we choose one of the most vulnerable attacks in the wireless sensor network that is sinkhole attack to study in details. Further, we reviewed all the existing routing protocol where the sinkhole attack can be generated and also described, how it can be incepted. Finally, we studied the survey paper that highlights the routing protocols prone to sinkhole attack.

Keywords: A Laptop Class Adversary; Gradient; Intrusion Detection System; Link Quality Estimates; Routing Protocol; Sinkhole Attack; Vulnerable;

I. INTRODUCTION

Wireless sensor network(WSN) is a collection of sensor nodes which are spatially distributed in the environment to monitor physical conditions such as sound, weight, temperature, etc. and to helpfully pass their information to the central location(Base station) through the network by using many well-known routing techniques. Base station is a computation center where all the computation has to be done. In WSN traffic flows in the direction ofthe base station through one or more sink nodes. WSN focuses mainly on sensing data, transferring the sensing data to the base station, which can manage all the communication between nodes. The potential applications of sensor network includes air traffic control, monitoring weather, traffic monitoring, automated and smart home, video surveillance and robot control, etc.

The predominant characteristics of WSN are distributed and wireless in nature. It also has many demanding constraints in the node battery power prevention. These imperatives make an extensive number of vulnerabilities that attacker can adventure to access the network [9]. Securing sensor arrange against these dangers is a testing research area. In WSN many routing protocols are not aware of these security issues and are not composed having security dangers as a main priority. So attacker need not put some extra effort to exploit the network and easily they can gain access to the network. So it is imperative to study the realistic routing protocols of WSN and to get to know how the attacker can essentially perform the attack.

The network layer is in charge of steering the information, provided by the transport layer. Many routing protocols are used to transfer the data or packets in the network between nodes. The network layer is vulnerable to a majority of attacks [8], [9] viz. selective forwarding, message flooding, sinkhole, black hole, worm hole and

Sybil attack, etc. Sinkhole attack is the most vulnerable attack in the network layer and intruder can easily exploit it [5]. In this manuscript, various sinkhole attacks are studied in detail.

In a sinkhole attack [5], the whole traffic of the network is attracted by the compromised node, which is responsible for the attack in the network. Compromised node cooperatively participates and is predominantly responsible for launching a sinkhole attack in the network. The traffic gets attracted by many methods like announcing a low hop count to the base station or an excellent connection to the base station and much more. The compromised node can alter the data packet, loss the data packet and it can also forward the data packet to the attacker. Sinkhole attack may be responsible for launching further attacks like select forwarding attack.

At long last, this paper researches a standout amongst the most vulnerable routing attacks that is sinkhole attack from assailant's perspective. So from this, we get to know the weakness of the routing protocols of WSN and trusting that this will prompt to a superior consciousness of era of the sinkhole attack. Hence, the study will also drive the improvement in routing protocols to enhance resistance to routing sinkhole attack.

There are many routing protocols those are vulnerable to sinkhole attack like MintRoute protocol, MultiHop LQI protocol, Tiny AODV protocol, TinyOS beaconing routing protocol, Directed diffusion(DD) routing protocol, and Rumor routing protocol, etc. Further, we will study these protocols in detail like their operation and the point of vulnerability to these attacks.

II. SINKHOLE ATTACK IN VARIOUS ROUTING PROTOCOL

2.1 MintRoute routing protocol [3],[4]

It is a new standard routing protocol for TinyOS.It's routing decisions mainly on link quality estimates rather than minimum hop count, to choose the best route to send a packet to the base station. Link quality estimation is calculated with the help of packet error rate. Each node appraises the connection nature of its neighbors in view of the loss ofpackets, which are received from their corresponding neighbor. Periodically, each node broadcast all these estimates for each neighbor in the form of packets, which is known as "route update packets". Every node keeps a neighbor table which is updated by the assistance of "route update packet". The neighbor table incorporates id's of every neighboring node and their comparing link cost. The node picks it's "parent node" to be the one with best connection quality in the neighbor table. On the off chance that two nodes have same connection quality then the minimum hop distance of each neighbor to the base station is thought about in picking the parent.

On the off chance that either the connection nature of at least one nodes gets to be distinctly 75% superior to the connection nature of the present parent or the connection nature of the present parent drops beneath 25 in total qualities, then the parent changing mechanism is activated, and the node with the most noteworthy connection quality turns into the new parent. In the event that two nodes have same connection quality then which one have least hop count to the base station will turn into a parent. In this protocol, the routing metric is Link estimates of links.

Attack: The sinkhole attack is launched with the help of compromised node. Compromised node removes current parent of nodes and makes sinkhole node as a new parent of nodes. The compromised node can launches sinkhole attack in two ways

1) Publicize an attractive connection quality for itself into the network.

2) Make other nodes appear as though they have more awful connection quality than itself.

This protocol doesn't permit the nodes to change their parents as often as possible, so the publicizing a high connection quality to the other node is not a smart thought. For that try another way to launching a sinkhole node that makes current parent link quality unsubstantial, so from this the parent changing algorithm will start in their children nodes. The new parent turns into the sinkhole node by modified the connection quality estimates sent by the parent nodes inside their "route update packet". The intruder will read the "route update packets" from its neighbor, modify them and replays them mimicking the original sender.

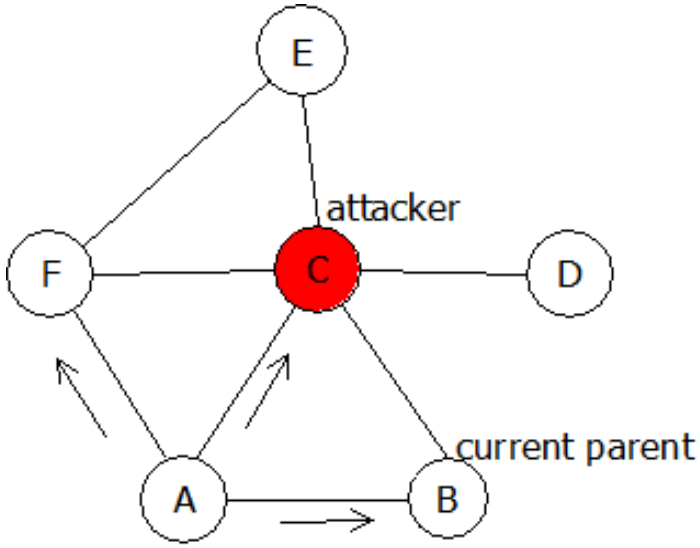

Fig. 1: Node C gets the "route update packet" of node A

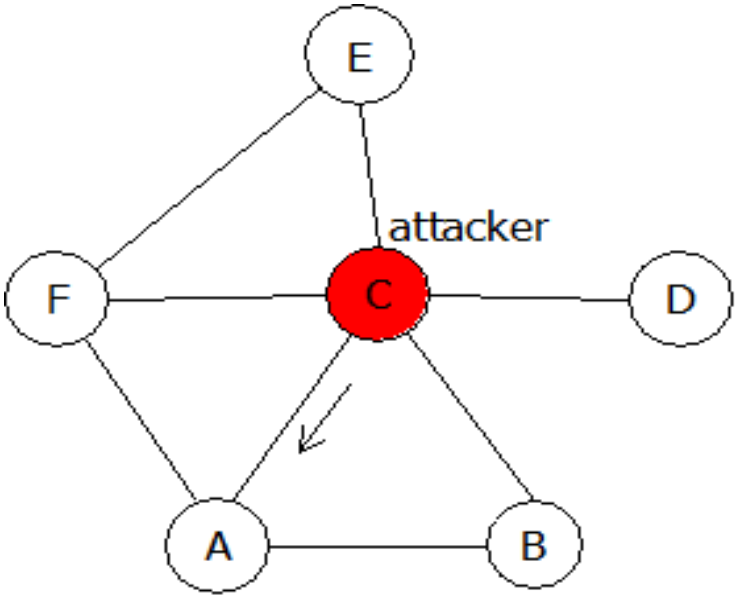

Fig. 2: Node C sends a malicious packet to node A imitating as node B

Table 1: Neighbor table of Node A

Node	Connection quality
B	170
C	255
F	150

Table 2: Updated neighbor table of node A

Node	Connection quality
B	20
C	255
F	150

First node A sends route update packet to node F, C, B (Fig. 1). Here the attacker is node C, and the current parent is node B (Fig. 1). Node C has sent its "route update packet" promoting a fake connection quality (most esteem 255), however this is insufficient to roll out node A to modify its parent (Table 1). In this way, when node C gets the "route update packet" of node A than it adjust the connection nature of node B to low esteem and sent back to node A. The node A again re-estimates the connection nature of all neighbor nodes and refresh the neighbor table (Table 2) correspondingly and furthermore apply parent changing algorithm. Since the connection nature of node B is bellow 25 (Table 2) so node B is ignored by node A and node C is picked as a new parent.

2.2 MultiHop LQI routing protocol [3],[6]

In this protocol, the connection quality is figured by the assistance of their hardware(Radio chip). Every node intermittently communicate a message (Beacon message) to the network, and the collectors separate the connection quality given by radio chip. This link quality is input to the function, and the function output is the cost of the corresponding link. Here, the link quality of the link is inversely proportional to the cost of the link.

Beacon message incorporates sender's present parent and the cost of the entire way to the base station (way cost). We can represent the cost of node A to node B as follows

$COST_{AB}$: cost estimation of node A that is connected to the node B.

Computation of path cost for a node B that has parent D is as per the following:

$COST_B = COST_{BD} + COST_D$

Node A read beacon message and stores the incentive in its table. It likewise ascertain the way cost to the goal as depicted previously.

Attack: There are mainly two ways to launch a sinkhole attack by an attacker

Way1: Promote a low way cost with its parent.

Way2: Make other nodes appear as though they have more regrettable way costs than itself.

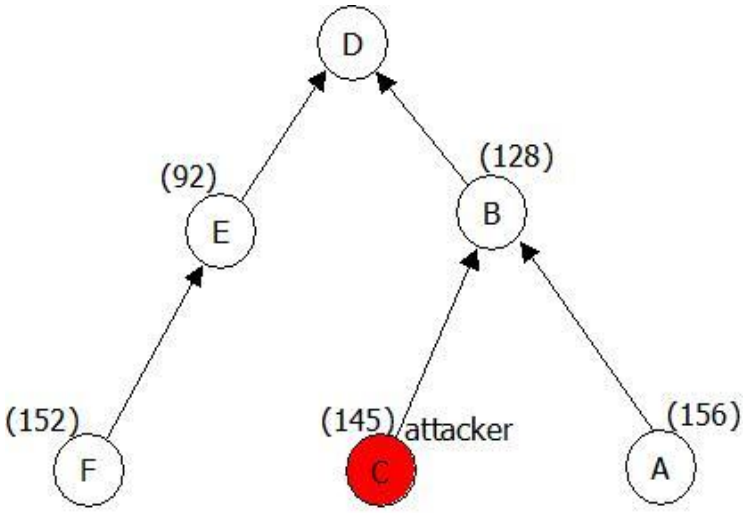

Fig. 3: Multi hop LQI routing protocol

Way1: The way cost that relates to the maximum LQI is 15. Node C reduces its path cost 145 to 15 (Fig. 4). Therefore node A, E, F changes their parent to node C (result of way1 attack) and the parent changing mechanism is also started at the parent (node B) of the attacker (node C) (Fig. 4).

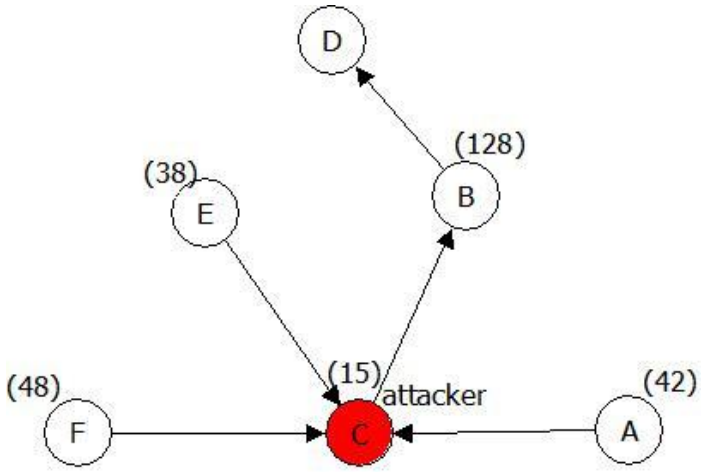

Fig. 4: Way 1 of attack

Way2: Attacker (node C) alter the path cost of node E is very high let's say, 1000. So from this node E's child (node F) estimates the path cost and realizes that it have very worse path cost in the way of node E (Fig. 5). So node F starts parent changing mechanism and choose node C (attacker) as its new parent (Fig. 5). On the off chance that the attacker (node C) takes a similar procedure for every hub, then it will able to attract all the traffic.

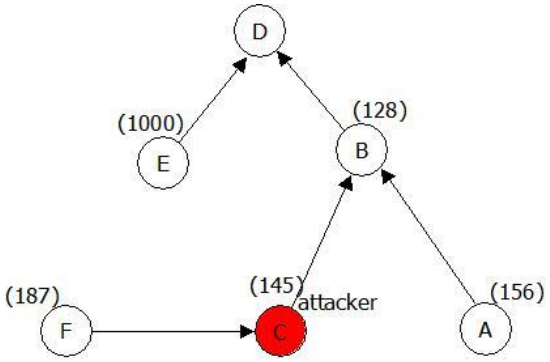

Fig. 5: Way 2 of attack

2.3 Tinoy AODV protocol [4],[6],[7]

TinyAODV is same as AODV in MANET, but TinyAODV is very lighter routing protocol compare to AODV in MANET [9]. AODV stands for ad-hoc on demand vector. In this protocol routing metric is the number of hopes to the base station.

When one of nodes needs to convey or needs to make an impression on the base station, first it need to make a way from source to destination so for that it sends RREQ (Route Request) packet to its neighbors. From that point onward, the neighbor node which is near the destination will send RREP (Route Reply) packet to the source node. At long last, the source node gets RREP packet from the neighbor and chooses one node with a minimum number of hop count to the destination.

Attack: The sinkhole attack can be generated by the help of compromised node. Compromised node will send RREP packet to the source node and inform to source node that it has a minimum number of hop count to the destination. Next, the source node decides to send packet to sinkhole node or compromised node. Compromised node performs the same technique to all its neighbors and attract as much traffic as it can.

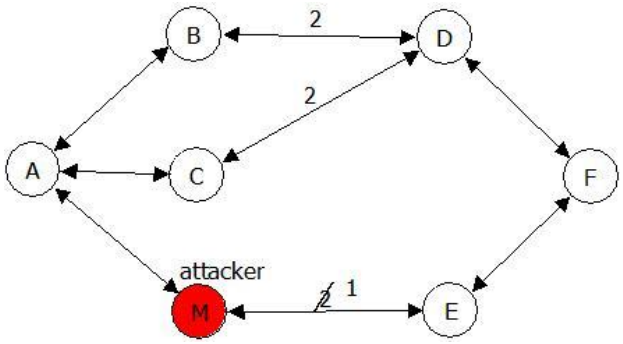

Fig. 6: Sinkhole attack in Tinoy AODV protocol

In Fig. 6 node A send routes request to node B, C, M. Node M is compromised node. Node B and C are sending packets to node D which is 2 hop distance far from the destination node. Compromised node M, which is 2 hop count far from destination node changes its 2 hop count to 1 hop count and send this updated information to node A in the form of RREP packet. Node A then rejects the path to the destination through node B, C and chooses a new path to the destination through node M (compromised node).

2.4 TinyOS beaconing [1],[2],[5]

This protocol constructs a spanning tree as the base station is the parent for all nodes. Occasionally base station communicate the "routing update packet" to its neighbors, and the neighbor nodes will communicate to its neighbors. This process is keep going on recursively until the routing update packet of the base station will not spread in the entire network. All packets received or produced by nodes are sent to their parent until they don't reach at the base station.

The straight forwardness of this protocol makes it defenseless to the sinkhole attack since routing updates are not verified and not authenticated as well. It is conceivable that any node can guarantee that it is the base station and can turn into the parent of all nodes in the network. Authenticated routing updates may tackle this issue, yet at the same time sinkhole attack can be created.

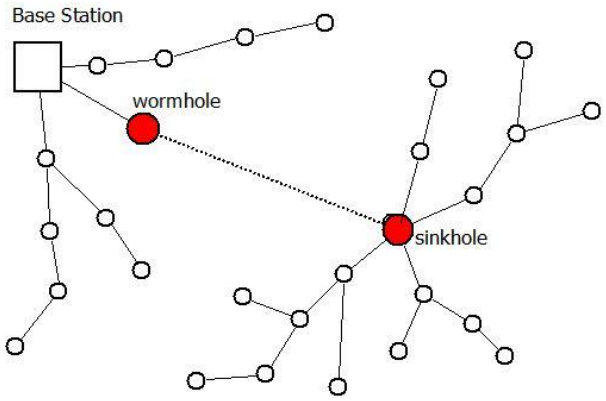

Fig. 7: A laptop class adversary utilizing a wormhole to make a sinkhole

Attack: In this protocol, the sinkhole attack is produced by the assistance of wormhole attack (Fig. 7). So for that, adversary first make a wormhole between two colliding laptop class nodes. One laptop class is close to base station, and other is close to focused attack region (Fig. 7). The primary node send authenticated routing update to the second node that is situated in focused attack zone through the wormhole. Further, the second node broadcast this packet to the focused attack zone. The second node creates a large routing sub tree in the focused attack zone with itself as the root (sinkhole) of that tree.

2.5 Directed Diffusion [1],[2],[5],[7]

This protocol is mainly used for distributed activates. It has two primary elements which are gradients and interest. Interest is a task description to define sensor events. It has a list of attributes including type, region, rate, span, and time stamp. Type is utilized to distinguish what kind of information is detected. The region is utilized to decide the network part from which information is drawn. The rate is utilized to distinguish, how frequently information is sent in the network. Span is utilized to decide, to what extent the interest ought to be dynamic. The time stamp is utilized to revive the interest. Each interest section has a few gradients to each neighbor node. Every gradient additionally has an arrangement of characteristics including a node identity (to whom the information needs to forward), data rate (how frequently the information is sent) and span (to recognize, to what extent the interest ought to be dynamic).

The fundamental work of this protocol to diffuse the interest in the network, setting up the gradients (slopes), sending information and path reinforcement. Every node that gets the interest will build a gradient towards the inception node. Gradient contains attribute value and direction.

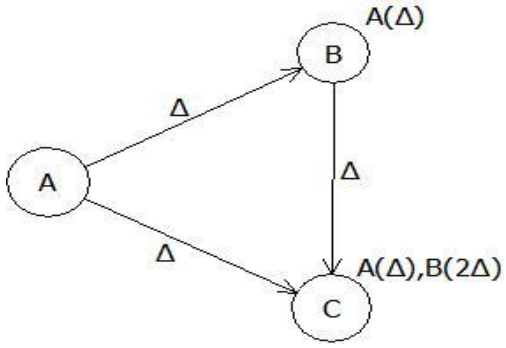

Fig. 8: Gradient setup in directed diffusion routing protocol

At the point when node B gets interest from node A, it incorporates A (Δ) as its gradient (Fig. 8). At the point when node C gets interest from node A through node B, it incorporates B (2Δ) as its gradient (Fig. 8). At the point when the information coordinates the interest (event), way data streams to the base station at a low rate then the base station recursively reinforces at least one neighbors to answer at a higher information rate.

In this protocol eavesdrop of the interest is an easy task. When adversary receives an interest from the network, it can only reply that interest with himself listed as the base station. The response is sent to the network and also received by the adversary.

Attack: a laptop class adversary can create a wormhole between one node near to base station and another node in the targeted attack area. The interest publicized by the base station and tunnels through the wormhole to the focused attack area. So the information streams far from the base station and towards coming about sinkhole.

2.6 Rumor routing [2],[5]

Rumor routing is a variation of directed diffusion routing protocol. In this protocol flooding is not used in the entire network to match the information, so we can say it is energy efficient routing protocol compare to Directed Diffusion routing protocol. This protocol is described by events, queries, and agents. The event is a marvel happening in a settled region of the network. Queries are requested for information to the nodes in the network. Agents are used to create paths leading to events. Agents are long-lived packet in the network. Every node in the way contains a list of its neighbors and event table. Event table incorporates name of the event, hop distance to an event and next node in the way towards the event. In this convention, any node can produce the query and afterward send it arbitrarily in the network to discover the way. The query keeps going until it finds the way or it's TTL (time to live) get to be distinctly zero.

At the point when a source node watches an event, then it creates an agent. The agent is broadcasted in the entire network to create the path leading to an event. Agent packet incorporates a list of all possible events, next possible path to those events, the hop distance of that path, a list of nodes that are previously visited and TTL field. If the base station wants to propagate query in the network so first, it creates an agent and then broadcast it into the network.

Attack: As explain above, the agents carry very sensitive information. So adversary can remove event information carried by the agent and forward to the attacker. Mote class adversaries can create sinkhole by extending tendrils in all the directions. It produces tendrils by forwarding multiple copies of a received agent.

III. CONCLUSION

We have illustrated that some proposed routing protocols are vulnerable to sinkhole attack in the WSN. Further, we proposed the generation mechanism of sinkhole attack in various existing routing protocols of WSN. So these routing protocols are unreliable and unsecure against sinkhole attack. Finally, we leave it as an open problem to design a sensor network routing protocols that satisfies our proposed security goals and possess prevention measures against sinkhole attack.

REFERENCES

[1] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2 (2003): 293-315.

[2] Sadeghi, Mohammad, et al. "Security analysis of routing protocols in wireless sensor networks." International Journal of Computer Science Issues 9.1 (2012): 465-472.

[3] Krontiris, Ioannis, Thanassis Giannetsos, and Tassos Dimitriou. "Launching a sinkhole attack in wireless sensor networks; the intruder side." Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,. IEEE, 2008.

[4] Kibirige, George W., and Camilius Sanga. "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network." arXiv preprint arXiv:1505.01941 (2015).

[5] Qureshi, Muhammad Danish, et al. "Analysis of Various Attacks in Routing Protocols for Wireless Sensor Network."

[6] John, Celia, and Charu Wahi. "Security Analysis of Routing Protocols for Wireless Sensor Networks." International Journal of Applied Engineering Research 11.6 (2016): 4235-4242.

[7] Hasan, Mohammed Zaki, Hussain Al-Rizzo, and Fadi Al-Turjman. "A Survey on Multipath Routing Protocols for QoS Assurances in Real-Time Wireless Multimedia Sensor Networks." IEEE Communications Surveys & Tutorials (2017).

[8] Shahzad, Furrakh, Maruf Pasha, and Arslan Ahmad. "A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures." arXiv preprint arXiv:1702.07136 (2017).

[9] Nazir, Muhammad Kashif, Rameez U. Rehman, and Atif Nazir. "A Novel Review on Security and Routing Protocols in MANET." Communications and Network 8.04 (2016): 205.

[10] L. Zhou and 2. Haas, "Securing ad hoc networks:' IEEE Newark Magazine, vol. 13. no. 6. November/December 1999.

[11] C. lntanagonwiwat, R. Govindan, and U. Estrin. "Direcled diffusion: A sealable and robust wmunication paradigm for sensor networks," in Proceedings of the Sixth Annul lntemtionnl Confit" on Mobile Computing and Neworks (MobiCOU 'XJJ, August 2000.

[12] Yick, B. Mukherjee, and D. Ghosal., Wireless Sensor Network Survey, 2008.

[13] J. Paul Walters, Z. Liang, W. Shi, and V. Chaudhary, Wireless Sensor Network Security: A Survey, Department of Computer Science Wayne State University.

[14] D. Braginsky and D. Estrin, Rumour routing algorithm for sensor networks, in First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[15] Abhishek Pandey and R.C. Tripathi. (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2.

[16] Choi, G. B., Cho, J. E., Kim,H. J., Hong, S. C. and Kim, H. J. (2008).A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In ICOIN (pp.1-5).

[17] David Martins and Hervé Guyennet. (2010) Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey, In Network-Based Information Systems (NBiS), 2010 13th International Conference on (pp. 313-320). IEEE.

[18] Ngai, E., Liu, J. and Lyu, M. (2006). On intruder detection for Sinkhole attack in Wireless Sensor Network. In Communications, 2006. ICC'06.IEEE International Conference on (Vol. 8, pp.3383-3389). IEEE.

[19] John Paul Walters et al, A Survey: ―Wireless Sensor Network Security‖ , Department f Computer Science Wayne State University, August 2008.

[20] K Lakshmi, S Manju Priya, A Jeevarathinam, K. Rama, K. Thilagam, " Modified AODV Protocol against Blackhole attacks in MANET", International Journal of Engineering and Technology.

[21] Seryvuth Tan, Keecheong Kim, " Secure Route Discovery for Preventing Blackhole Attacks on AODV Based MANETs" IEEE International Conference on Telecommunication, 2013.

[22] Dutta, C.B. ; Dept. of CSE, Univ. of Kalyani, Kalyani, India ; Biswas, U. A novel blackhole attack for multipath AODV and its mitigation, Recent Advances and Innovations in Engineering (ICRAIE), 2014.

[23] Khan, Shafiullah, et al. "Passive security threats and consequences in IEEE 802.11 wireless mesh networks." 2; 3 (2008).

[24] F. Akyildiz et al., "A Survey on Sensor Networks," IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–14.

[25] Garg, N., Aswal, K. and Dobhal, D.C. (2012) A Review of Routing Protocols in Mobile Ad Hoc Networks. International Journal of Information Technology, 5, 177-180.

[26] de Morais Cordeiro, C. and Agrawal, D.P. (2002) Mobile Ad Hoc Networking.

[27] C. Jisul and K. Keecheon, "EADD: Energy aware directed diffusion for wireless sensor networks," International Symposium on Parallel and Distributed Processing with Applications (ISPA) , pp. 779-783, 2008.