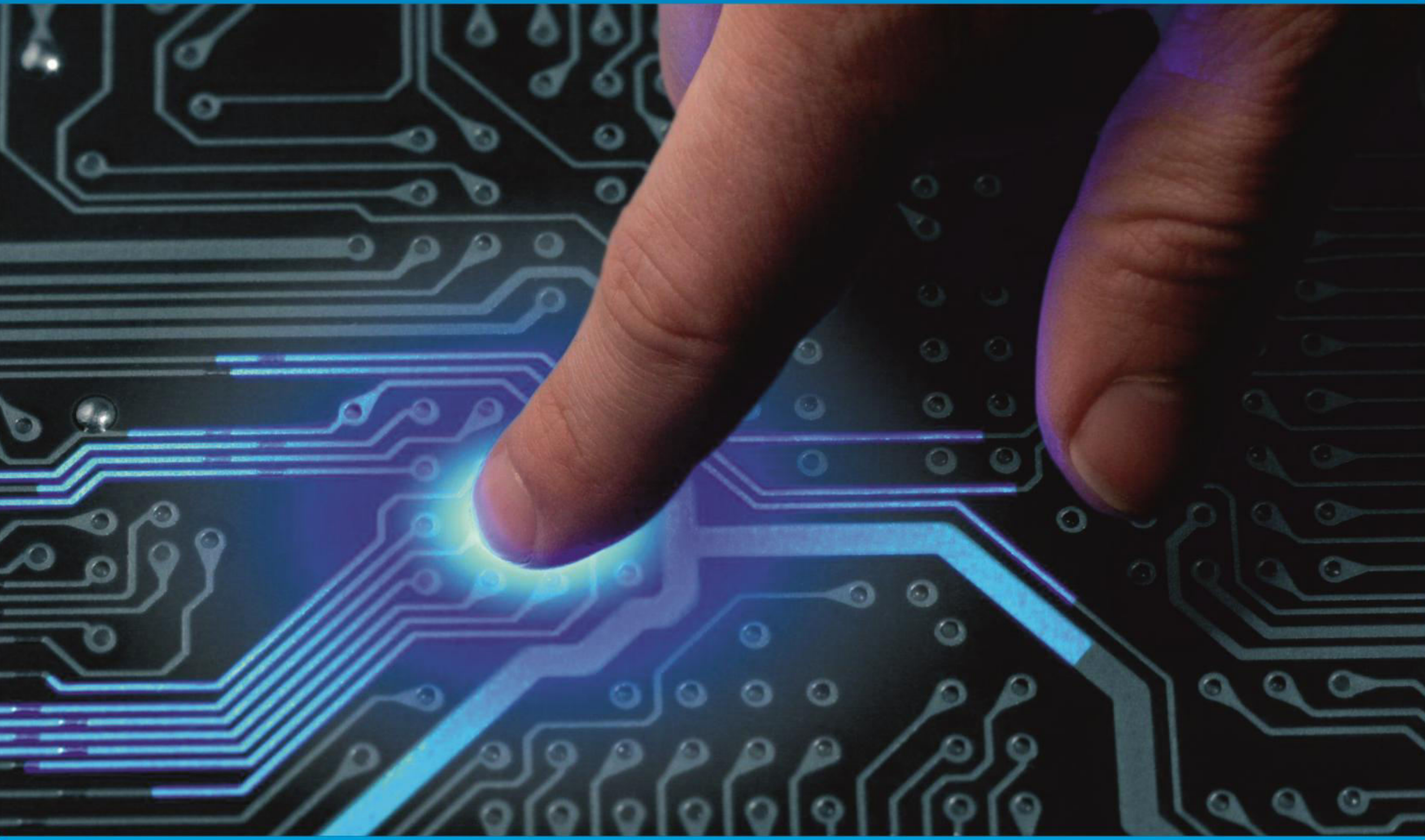
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| DOI: 10.15680/IJIRCCE.2021.0905143|

Effective Framework against Sinkhole Attack Using TMCRP

D.Vennila, K.Mathi Poorani, G.Jency Jose, Mrs.V.Lavanya

UG Student, Dept. of CSE, Velammal College of Engineering and Technology, Madurai, Tamilnadu, India

Assistant Professor, Dept. of CSE., Velammal College of Engineering and Technology, Madurai, Tamilnadu, India

ABSTRACT: Wireless Sensor Network (WSN) consists of large number of low-cost, resource-constrained sensor nodes. The constraints of the wireless sensor node is their characteristics which include low memory, low computation power, they are deployed in hostile area and left unattended, small range of communication capability and low energy capabilities. Base on those characteristics makes this network vulnerable to several attacks, such as sinkhole attack. Sinkhole attack is a type of attack were comprised node tries to attract network traffic by advertise its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. It can also used to send bogus information to base station. This paper is focus on exploring and analyzing the existing solutions which used to detect and identitfy sinkhole attack in wireless sensor network. The analysis is based on advantages and limitation of the proposed solutions.

KEYWORDS: Wireless sensor network (WSN), sinkhole attack, detection of sinkhole attack

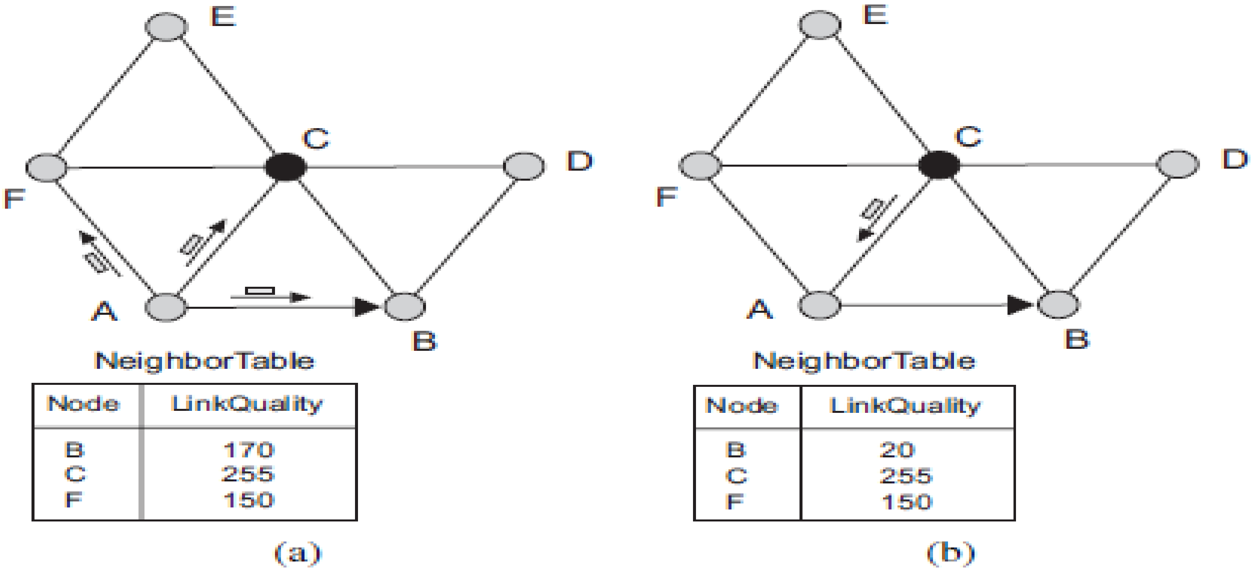
I. INTRODUCTION

Wireless sensor network consists of small nodes with ability to sense and send data to base station [5]. Wireless sensor network is used in different applications example in military activities, which used to track movement of their enemy. It also used in fire detection and in healthy service for monitoring heart beat [2, 17, 3]. Unfortunately most of wireless network are deployed in unfriendly area and normally left unattended.Also most of their routing protocols do not consider security aspect due to resource constraints which include low power supply and low communication range [8,9]. This constraint creates chance for several attackers to easily attack wireless sensor network. An example of attack is sinkhole attack. Sinkhole attack is implemented in network layer where an adversary tries to attract many traffic with the aim to prevent base station receiving a complete sensing data from nodes [20]. The adversary normally compromises the node and that node will be used to launch an attack.

II. SINKHOLE ATTACK

Sinkhole attack is an insider attack were an intruder comprise a node inside the network and launches an attack. Then the compromise node try to attract all the traffic from neighbor nodes based on the routing metric that used in routing protocol. When it managed to achieve that, it will launch an attack. Due to communication pattern of wireless sensor network of many to one communication where each node send data to base station, makes this WSN vulnerable to sinkhole attack (Ngai et al[18]).

The following subsections discuss the techniques use in MinRoute protocol and AODV protocol in launching sinkhole attack.



NeighborTable

Node	LinkQuality
B	170
C	255
F	150

NeighborTable

Node	LinkQuality
B	20
C	255
F	150

Figure 1 : Sinkhole attack in MinRoute

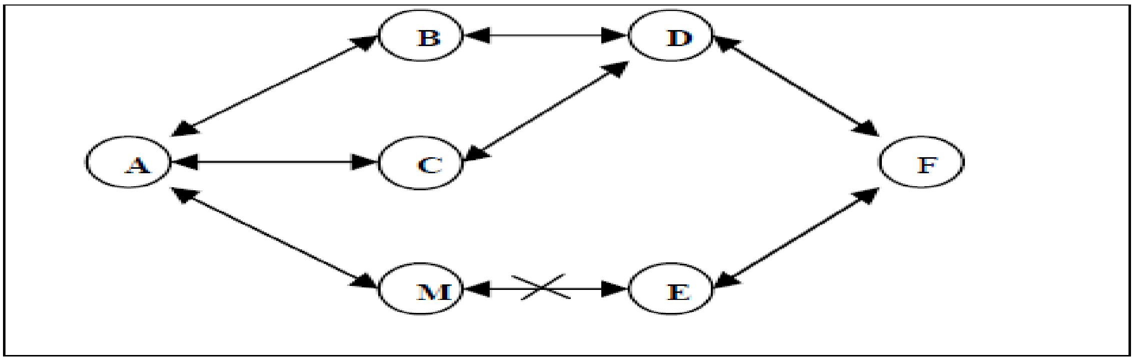


Figure 2 : Sinkhole attack in MintRoute protocol (Krontiris, I[15])

Sinkhole Attack in MintRoute Protocol

MintRouteprotol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network, it is light and suitable for sensor nodes which have minimum storage capacity, low coputation and limited power supply. MintRoute protocol uses link quality as a metric to choose the best route to send packet to the Base Station (Krontiris et al [15]).

Fig. 1 shows six sensor nodes A, B, C, D, E, and F. Node C is malicious, and it is going to launch a sinkhole attack. The figure 1(a) shows a route table of node A with IDs of its neighbors with their corresponding link quality. Orginallly the parentnode with node B but node C advertises its link quality with a value of 255 which is maximum value. Node A is not going to change its percent node until the node B's link quality fall to 25 below the absolute value.

In Fig. 1(b) the malicious node is sendin new update route packet that the link quality fall up to 20 and impersonate node B so that node A believe thepacket come from node B. Node A will update its routetable and change the parent node to node C (Krontiris et al [15]). The attacker uses node impersonation to launch anattack.

Sinkhole Attack in TinyAODV Protocol

This is another explanation of sinkhole attack in wireless sensor network and this time the attack is launched under TinyAODV (Ad-hoc On Demand Vector) protocol. TinyAODV protocol is the same as AODV in MANET but this one is lighter compared to AODV and it was modified purposely for wireless sensor network [27]. The number of hops to base station is the routing metric that used in this protocol. Generally the route from source to destination is created when one of the nodes send a request, the source node sends a RREQ (Route request) packet to his neighbors when wants to send packet. Next oneof the neighbors close to destination is reply by sending back RREP (Route Reply) packet, if not the packet is forwarded to other nodes close to thatdestination.
Finally, the source receives RREP packet from neighbor then select one node with less number of hops to destination.

The sinkhole node or compromised node launches an attack by send back RREP packet. In RREP packet it gives small number of hops which indicates close proximity to the base station. Then the source node decides to forward packet to sinkhole node. The comprised node then performs the same technique to its entire neighbors and tries to attract as much traffic as possible [27].

For instance, Fig.2 shows node M launches sinkhole attack in Tiny AODV. Node A sends RREQ to nodes BCM. However node M instead of broadcast to node E like nodes B and C does to node D, he replies back RREP to node A. Then node A will reject node B and C, then forward packet to M because node A and B are very far to F compare to node M.

III. CHALLENGES IN DETECTION OF SINKHOLE ATTACK IN WSNs

Based on the literature review of sinkhole attack in Wireless sensor network, the following are the main challenges in detecting sinkhole attack in wireless sensor network.

A. Communication Pattern in WSN:

All the messages from sensor nodes in wireless sensor network are destined to base station. This created opportunity for sinkhole to launch an attack. Sinkhole attacks normally occur when compromised node send fake routing information to other nodeskin the network with aim of attracting as many traffic as possible. Based on that communication the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenges because the communication pattern itself provides opportunity forattack.

B. Sinkhole attack is unpredictable:

In wireless sensor network the packet are transmitted based on routing metric that used by different routing protocols [2]. The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack.Then all the data from his neighbors to base station will pass through compromised node. For example the techniques used by compromised node in network that used TinyAODV protocol is different to the one used another protocol like MintRoute protocol. In MintRoute they used link quality as route metric while in Tiny AODV they used number of hop to base station as routing metric. Therefore the sinkhole attack techniques is changed based on routing metric of routingprotocol.

C. Insider Attack:

Insider attack and outsider attack are two categories of attack in wireless sensor network. Outside attack is when intruder is not part of network. In inside attack the intruder comprises one of the legitimate node through node tempering or through weakness in its system software then compromised node inject false information in network after listen to secret information. Inside attack can disrupt the network by modifying routing packet. Through compromised node sinkhole attack attract nearly all the traffic from particular area after making that compromised node attractive to other nodes. The fact is that compromised node possesses adequate access privilege in the network and has knowledge pertaining to valuable information about the network topology this created challenges in detecting.

D. Physical attack:

A wireless sensor network normally deployed in hostile environment and left unattended. This provides a opportunity for an intruder to attack a node physically and get access to all necessary information [12].

IV. EXISTING APPROACHES

Many researchers have been working on wireless sensor field to provide security mechanism to suits the resource constrained due to growing demand of applications in sensitive areas. The following are the identified approaches that used by different researchers to detect and identified sinkhole attack in wireless sensor network. Those approaches are classified into rules based, key management,anomaly based, statistical method and hybrid based. The subsequent subsections described each of these categories and give examples of existing work that used thatapproach.

A. Rule based

The rules are designed based on the behavior or technique used to launch sinkhole attack. Then those rules are imbedding in intrusion detection system which runs on each sensor nodes. Those rules were then applied to the packet transmitted through the network nodes. If any node violates the rules is considered as adversary and isolated from the network.Among the existing work which used rules based approach include Krontiris et al [14]. Krontiris used Rule based approach to detect sinkhole attack. They create two rules and implanted in Intrusion detection system (IDS). When one of the rules is violated by one of the nodes, the intrusion detection system triggered an alarm but it does not provide node ID of compromised node. The first rule “for each overhead route update packet the ID of the sender must be different your node ID”. The second rule “for each overhead route update packet the ID of the sender must be one of the node ID in your neighbors”. AlsoKrontiris et al [15] used the same approaches. There are two rules, the first rule “rule for each overhead route update packet the ID of the sender must be one of node ID in your neighbors”. The second rule “for each pair of parent and child node their link quality they advertise for the link between them, the difference cannot exceed 50.

B. Anomaly-based detection

In anomaly based detection the normal user behavior is defined and intrusion detection is searching for anything that is anomalous in the network. In this method intrusion is considered as anomalous activity because it looks abnormal compare to normal behavior. The rule based and statistical approaches are also included under anomaly based detection approach.

Tumrongwittayapak and Varakulsiripunth [29] proposed system that used RSSI (Received Signal Strength Indicator) value with the help of EM (Extra Monitor) nodes to detect sinkhole attack. The EMhad high communication range and one of their functions is to calculate RSSI of node and send to base station with ID of source and next hop. This process happens instantly when node are deployed. Base station uses that RSSI value to calculate VGM (visual geographical map). That VGM shows the position of each node, then later when EM send updated RSSI value and base station identify there is change in packet flow from previous data this indicate there is sinkhole attack. The compromised node is identified and isolated from the network by base station using VGM value. However, if attack is launched immediately after network deployment, the system will not be able to detect that attack [29]. Also the numbers of EM nodes were not specified for specific number of sensor nodes and the proposed method is focused only on staticnetwork.

C. Statistical method

In statistical approaches the data associated with certain activities of the nodes in network is studied and recorded by researchers. For example monitor the normal packet transmitted between the nodes or monitor resource depletion of the nodes like CPU usage. Then the adversary or compromised node is detected by comparing the actual behavior with the threshold value which used as reference, if any nodes exceed that value is considered as an intruder.

Chen, et al [3], proposed statistical GRSh (Girshick- Rubin Shyriaev)–based algorithm for detecting malicious nodes in wireless sensor network. Base station calculates the difference of CPU usage of each node after monitoring the

CPU usage of each node in fixed time. Base station would identify whether a node is malicious or not after comparing the difference of CPU usage with the threshold.

Dynamic trust management system was proposedby Royetal[23]todetectandeliminatemultipleattacks such as sinkhole attack. Each node calculates the trust of its neighbor node based on experience of interaction; recommendation and knowledge then send sto basestation. Thebasestationdecidedwhich node is sinkhole after it received several trust values from other nodes. Therefore the trust value of the node which falls beyond the normal value 0.5 is considered as sinkhole attack[23].

D. Hybrid based intrusiondetection

The combination of both anomaly and signature based or misused based is used in this approach.The falsepositiveratewhichproducedbyanomalybased is reduced in this approach due to the use of both method. Also the advantage of this approach is to be able to catch any suspicious nodes which their signature is not included in detectiondatabase.

Coppolino and Spagnuolo [6] proposed hybrid Intrusion detection system to detect sinkhole attack and other attacks. They used detection agent which was responsible for identifying was attached to sensor node and share resource of that node. The suspicious nodes were inserted to the blacklistbased on anomalous behavior after analyzed the collected data from neighbors. Then that list is sent to central agent to make final decision based on feature of attack pattern (misused based). Similar to solution proposed by Tumrongwittayapak and Varakulsiripunth [29], it was designed for static wireless sensornetwork.

E. Key management

In key management approach the integrity and authenticity of packet travels within the network is protected by using encryption and decryption key. Any packet transmitted in the network is added with another message in a way that to access that message requires a key and any small modification of the message can be easily detected. Those keys also help nodes to check if the message comes from basestation and check the authenticity of the message.

Papadimitriou et al [21] proposed a cryptographic approach in routing protocol to address the problem of sinkhole attack. Each node obtained public key which used to verify if the message comes from base station. They also used pair of public and private keys for authentication and sign data message. All keys were uploaded offline before the network was deployed. Their techniques prevented any node to hide its ID and any packet forgery between nodes in the network. This protocol is focused on resistance to sink hole attack but not to detect and eliminate it.

Meanwhile, Fessant et al [10] proposed two protocols which used cryptographic method to increase the resilience of sinkhole attack. Both protocols prevent malicious node from lying about their advertised distances to base station. However, they did not show the memory usage of their protocols and message size.

The summary of existing works using the previously described approaches is shown inTable 1.The summary covers evaluation results of proposed solution and their limitations.

Table 1: Existing works on Sinkhole detection

Approach	Proposed Solution	Result	Limitations/Advantages
Rule Based. Krontiris et al 2007 [16]	They extended their IDS which can detect sinkhole attack.	• the success of intrusion detection system dependon the increase number of watchdog • When the network density increase the false negativerate decrease.	Limitations • Memory and networkoverhead wascreated. • They used MintRouteprotocol • Node impersonation was the focus of therules. Advantages • More secure and robustmeasure can be developed based on valuable principle theydevelop.
Rule Based. Krontiris et al 2008 [15]	They proposed detection rules that will keep aware legitimate node the existing of attack.	• They show howvulnerabilities of MultihopLQI can be exploited by sinkhole node and suggest the rules which make the protocol more resilient.	Limitation • They did not showpractically how those rules can prevent attack. • All the rules are onlydetecting attack but cannot give ID of sinkhole node. • They assume attacker has the same power as normal nodeand can capture sensor node and change the internalstate.
Anomaly based. Tumrongwittayapak, C and Varakulsiripunth, R 2009 [29]	They proposed detection solution based on received signal strength indicator(RSSI) Their proposed solution required support from extra monitor node	• For 0 to 40% percentage of message drop the detection rate is100% • False positive rate was 0 for 0-40% of message drop but increase when percentagedrop increase • The same applied to false negative rate with themore message drop the more negativerate.	Limitation • They assume sensor networkare static • No instant attack • Base station remain 0,0position • Base station and extra monitor node are physicallyprotected. • Their proposed solution can notdetect attack if it happened instantly after network deployment.

Anomaly based. Choi et al 2009 [4]	They proposed method that can detect sinkhole attack that used LQI (link quality indicator).	• The probability of detection increase when number of detector nodes increase • detection rate increase when detector node increase • The false positive rate depend on extent of tolerance value (constant value which will show if changes is beyond abnormal)	Limitations • All sensor node have nomobility • The detection of sinkhole occurs when detector node is between sinkhole node and source node and sinkhole and basestation • The detector nodes have high source of energythan sensornodes Advantage • Detector nodecommunicate themselves through exclusivechannel
Anomaly based. Sharmila , S. and Umamah eswari, G.2011. [24]	-They proposed message digest algorithm to detect sinkhole node.	• The results show the algorithm worked well when malicious nodes are below 50% • False positive rate was 20%(due to packet drop) that figure obtained when malicious node reach50 • False negative error was 10% but was increasing when malicious node reach above 40	Limitation • Network throughput, overhead and communication cost was not calculated • The performance was not good when there is node collision, limited transmitted power and packetdrops • Only one advertisement is considered at a time, after computation another takeplace Advantage • The algorithmachieve data integrity and authenticity
Key Manage ment. Papadimi triou et al 2009 [21]	-They proposed two RESIST protocols which increase resilience to sinkhole attack inWSN	-Results show that RESIST-0 has high resilience to sinkhole attack (it does not allow node to lie about their distance to base station) than other protocol	Limitation • Resist-0 is very expensive it require two additional message to a packet • In their simulation message losses and collusion were notconsidered • Collusion node has impact on RESIST-0 not inRESIST-1

V. DISCUSSION

From the Table 1, it shows most approaches managed to detect and prevent sinkhole attack in WSN.Rule based approaches managed to detect sinkhole attack but it creates memory and network overhead. This approach did not give the ID of sinkhole node after detection of attack. All the rules focus on the node impersonation.

Anomaly based approach also manage to detect sinkhole attack but they just focus on static wireless sensor network. This approach created high false positive rate when there was high message dropping.

Key management was another approach which focused on resistance to sinkhole attack but not to detect and eliminate it.

VI. CONCLUSION AND FUTURE WORKS

Based on existing works most researchers are tryingto look for ICT solutions for detecting, identifying and providing resistance to sinkhole attack in wireless sensor network. Researchers used intrusion detection scheme based on anomaly-method, other used rule based and key management to detect and identifying the sinkhole nodes. Majority of researches struggled with security challenges corresponding with availability of resources and mobility of wireless sensor nodes. Some provided solution for only static and few on mobile network. Very few researchers managed to validate their security system usingreal wireless sensor network. Also some of results showed low detection rate, high network overhead and high communication cost. The future solution should focus on reducing high network overhead, computational power, increase detection rate and that system must be validated in real sensor network. Through this kind of validation, it will be easy to check if their solutions meet the available resources of WSN, such as memory capacity.

ACKNOWLEDGE

We would like to thank almighty God for giving us strength during the all period of the research. We would to like to express our sincere appreciation to other colleague in our department for their advice.

REFERENCES

1. R. Dutta, P. H Pathak. “Centrality-based power control for hot-spot mitigation in multi-hop wireless networks” Computer Communications, 2012, 35(9): 1074- 1085.
2. Fouad El Hajji, CherkaouiLeghris, Khadija Douzi. “Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks” Journal of Communications and Information Networks, Vol.3, No.1, Mar. 2018 Posts & Telecom Press and Springer Singapore 2018.
3. Y. Gu, F. Ren, Y. Ji, et al. “The evolution of sink mobility management in wireless sensor networks: A survey” IEEE Communications Surveys & Tutorials, 2016, 18(1): 507-524.
4. G. P. Joshi, S. Y. Nam, S. W. Kim. “Cognitive radio wireless sensor networkapplications, challenges and research trends “ Sensors, 2013, 13(9): 11196- 11228.
5. V. Kumar, S. Kumar. “ Energy balanced position-based routing for lifetime maximization of wireless sensor networks “ Ad Hoc Networks, 2016, 52: 117- 129.
6. A. Sarkar, T. S. Murugan. “Routing protocols for wireless sensor network” Alexandria Engineering Journal, 2016, 55(4): 3173-3183
7. A. Sharaf, J. Beaver, A. Labrinidis. “Balancing energy and quality of aggregate data in sensor networks “ The International Journal on Very Large Data Bases, 2004, 13(4): 384-403.
8. A. Wichmann, T. Korkmaz. “Smooth path construction and adjustment for multiple mobile sinks in wireless sensor networks “ Computer Communications, 2015, 72: 93- 106.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING