Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 8, August -2017

# A Hybrid Approach to Resolve SinkHole Attack in WSN using RAEED and ADOV Protocols

Punnet Kaur, Navpreet Kaur

[1]*Computer Science and Engineering, Punjabi University Regional Centre for IT and Management Mohali*
*Computer Science and Engineering, Punjabi University Regional Centre for IT and Management Mohali*

**Abstract** — *MANET contains large number of resource constraints and low-cost sensor nodes. When data is transmitted through these sensor nodes the key concern of MANET is to establish a routing protocol. Sink Hole attack is the one of famed attack that can interrupt the data traffic by attracting the traffic toward itself and does not allow data to be transferred further. Many protocols and techniques are used to remove sinkhole attacks but they all have some drawbacks. In the previous work RAEED (Robust formally Analyzed protocol for wireless Sensor networks Deployment) protocol is used. To enhance the working of data transmission, combine the RAEED protocol with AODV protocol. The route is find through Artificial Bee colony. The proposed work hybrid two protocol and remove the sinkhole attack efficiently. In this work, simulate the proposed work on the basis of different criteria like number of Nodes, Average delay, Average Density and Time span. This Hybrid approach gives better results in various parameters like message lost, error rate, throughput and setup time.*

***Keywords***- *MANET, RAEED, AODV, KSP, ABC.*

## I. INTRODUCTION

Wireless Sensor Network is described by gathering of low price embedded devices or nodes that connect wirelessly in ad-hoc network. Mobile Ad hoc network (MANET) are the dynamic and self-configuring networks that have the de centralized system [1]. The devices in MANET are joined by wireless medium. The information is generated from source nodes and the intermediate node that sense information from environment and is broadcast wirelessly to node at destination. Due to low cost sensor devices in the hostile environment the immune of nodes is weak thus lots of attacks are deployed. The broadcast nature of transmission enhances the chances of attacks. One the famous category of attacks is Denial of Service attacks(DOS) [2,3].

The DOS attacks interrupt the routing when data is transmitted from source to destination node. DOS attacks are further categorized as Control traffic Attacks, Path DOS, Data traffic Attacks. Control traffic attacks disrupt the routers, liveness of nodes and discovery of topology. The main Control Traffic attacks are warm hole, hello flood, Sybil attacks and many more. In Data traffic Attacks, attackers force data nodes to drop the packets. They are blackhole attacks, selective and jamming etc. Control traffic attacks limited the resources to go forward. These are most difficult attacks to detect. One of the famous Control attack is sinkhole attack. This paper mainly focus on Sinkhole attacks and research techniques that ca easily remove the sinkhole attacks during data transmission. Sinkhole attack is the one of the most destructive routing attack for WSN network, it enables other attacks [4]. These attacks are difficult to discover by any protocol because the information supplied during data transmission to any node in the WSN is very difficult to verify. During the processing of sinkhole attack, the main aim of attacker is to trap the traffic from particular area in WSN network by using any compromised node. Sinkhole nodes tries to attract data(info) toward itself by convincing the neighbour nodes by broadcasting fake routing information.

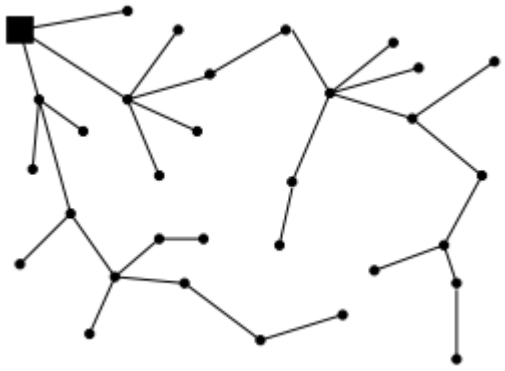

*Figure 1. A representative topology constructed using Tiny OS beaconing with a single base station.*

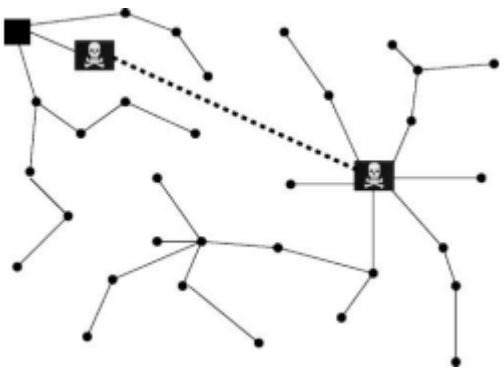

*Figure. 2. A laptop-class adversary to create a sinkhole in Tiny OS beaconing.*

 

A sinkhole attacks are mainly occurred in laptop with high range that resist to more hopes to other nodes, fake message near the base station indicating by a node, warm hole provided low latency and low hop distance link etc. thus the removal of Sinkhole attack is headache for every researcher. Fig. 1. Describes the representation topology that is constructed using Tiny OS beaconing with one base station while in Fig. 2. A sinkhole attacks is created in a laptop class in Tiny OS beaconing [5]. Many protocols are proposed to remove these attacks, but all them of them have some drawbacks. the routing protocols defined in policies that often govern the particular usage for endpoint provision for instruction packets. In MANET, many routing protocols used based on the situation of network. In the previous approach [6], RAEED protocol is used to control the sinkhole attack. The attacks are avoided by confirmed that the attackers failed to influence the routing information. All sensors and their neighbor's nodes in network were assigned at correct level. The previous work avoid Sinkhole attack but for better optimization and improvement in parameters the hybrid Approach of Protocols RAEED and AODV has been used in the proposed work. This approach not only avoid the sinkhole attack. The ABC algorithm has been used to find the route between source node and destination node for data transmission. The result evaluation will be done using following parameters Message Lost, Error Rate, Setup time, Throughput.

## II. RELATED WORK

Many scholars worked on WSN and MANET networks to offer the security mechanism when data transferred from source to destination. There are many techniques presented by many scholars to detect and control the sinkhole attacks in MANET [7]. In 2007[8], Krontiri et al. presented the rule based technique to avoid sinkhole attacks in WSN network. This paper scratched their IDs for detecting attacks that results in succeed of intrusion detection system and with value of network density increased the false negative rates decreased. The secure and robust network developed during this research. The main limitation of this research is network overhead and node imperfection. In 2009[9], Choi et al. presented Anomaly based method that used LQI (link quality indicator) to detect the sinkhole attack. With rise in detection nodes the probability of detection rate is amplified and false positive rate depends upon extent to tolerant value. The main benefit of this research is that detector sensors communicate through exclusive channel. But the limitation is that nodes have no mobility, detection of attacks like sinkhole is occurred when node is among between sinkhole node and base station. In 2007[10], Coppolino et al. presented the Hybrid base detection system that protect the critical data from direct attacks. It results in 3% false positive rate and 95-97% detection rate. The benefits of this approach contain the available resources and use anomaly method. In 2009[11], Papadimitriou et al presented a key management approach that introduced RESIST protocol that rises the elasticity to attacks. Then prevents the malicious sensors nodes from varying distance overhead node. But the RESIST approach is expensive. In 2016[6], Kashif Saghar explain the working of RAEED protocol to resolve the sinkhole attacks during data transmission. The RAEED protocol works in three stages KSP, RSP and DFP. The main limitation of this approach is that it doesn't consider routing table. For that reason, in the proposed approach the AODV protocol is combined with RAEED protocol. All the approaches that managed to identify, detect and provided resistance to sinkhole attacks. In next section protocols that used to improve the performance of sensor network while data is transmitted from source to base station are explained.

## III. METHODOLOGY

The proposed work is shown inFigure1(a). The simulation environment is created in MATLAB with having network properties, nodes and data. Input source node and destination node. The data is transmitted from source node to destination node. Then apply the Artificial Bee colony algorithm. ABC checks the neighbor nodes and their distance within coverage set. Then neighbor node act as source node and search for nodes within coverage set. This process continues until we find an accurate path between source node and destination node. Then the working of RAEED protocol comes into existence. RAEED have different phases and each phase have different functionality. The BVP phase is used for 3-way handshaking that is used for data transmission. The KSP is used to generate key that is for used for encryption process. The LPP is the phase in RSP that provides the time span and rebroadcast the message if message is not received by the received node. The RSP phase rectify the sink hole attack. Then encryption is used to encrypt the transmitted data. The key is generated during this process and encoded after the decryption is occurred. When data is received by neighbor node, it checks its entry in neighbor table. The DFP works along this process and remove the sinkhole attack. After this process AODV process is started. The AODV process start its processing and send the Hello message to all neighbor nodes. RREQ and RREP messages confirm the route from source to destination. At the end, the shortest Route is picket. ADD values in the neighbor table and select the node with less number of hop counts. When data is reached at the destination some parameters are calculated to evaluate the working of proposed work. Those parameters are Message Lost, error rate and throughput according to variations in number of nodes, delay, density and time span. Our proposed approach gives better results as compare to previous approach.

 

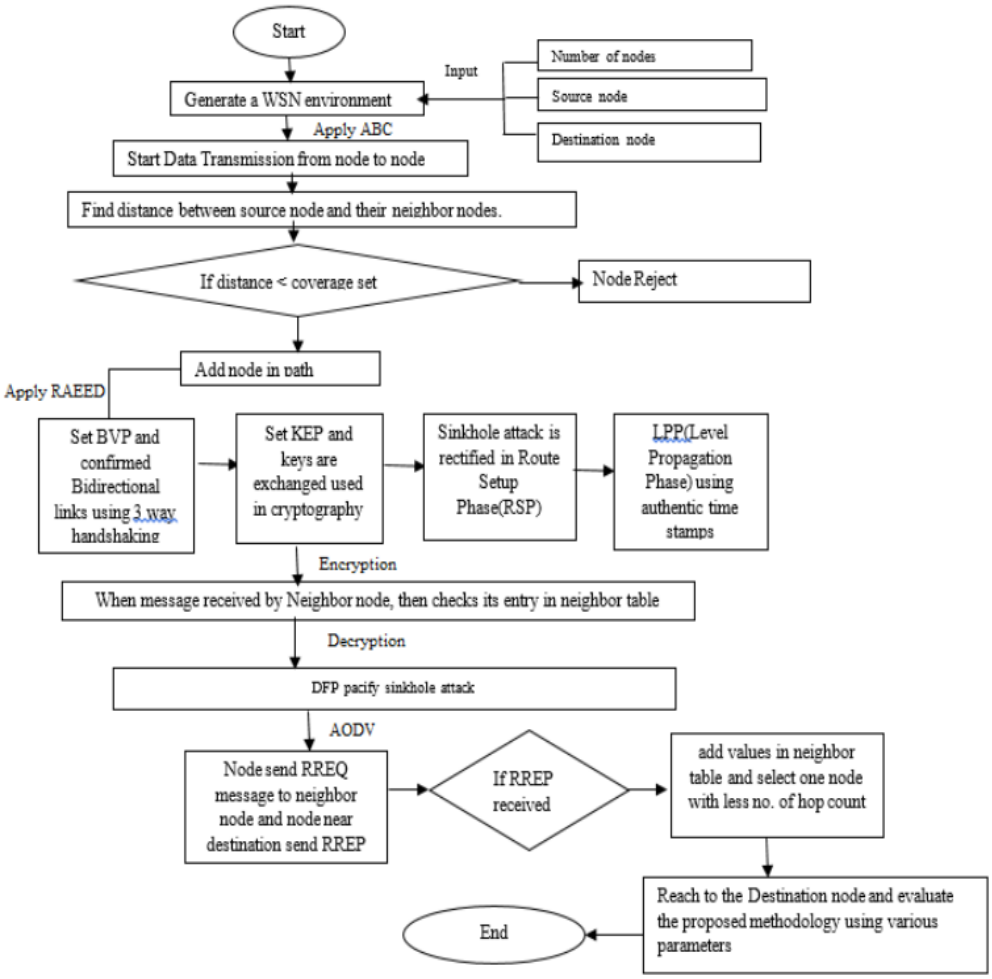


**Figure 3. Working of proposed work.**

## IV. IMPLEMENTATION AND PROTOCOLS

The RAEED and AODV protocols are combined to control the sinkhole attacks. These protocols have different functionality**.** These two protocols are compatible with each other. During implementation Sinkhole attack is control by RAEED protocol and then route is established by AODV protocol. These two protocols have some explanation as discussed below:

1. **RAEED**:
   RAEED is one of the powerful and stable protocol analysis that is implemented for WSN. RAEED is secure and more over powerful routing protocol [6,12]. The various phases of RAEED protocol is shown in Figure 3. RAEED have mainly work based on three stages: KSP, RSP and DFP. KSP is stage key setup phase and DFP is forward phase data. These stages are divided as:

   **A. Key Setup Phase (KSP)**

   KSP is the combination of two stages. First one is BVP (Bidirectional of documentation) and second one is KEP (exchange keys). In BVP (Bidirectional of documentation) 3-way handshake protocol is used to establish the bi-directional relationships between nodes. The main inspiration of this technique is to eliminate all unidirectional links between nodes, counting hi-flood attackers and in KEP is used for encryption in future stages of RAEED.

   **B. Route Setup Phase (RSP)**

   In RSP the two HOP that is ID-tied unit 1-HOP or 2-HOP road alignment exchange phase are explained. The neighboring nodes are checked during this process that are available in PSC. The pebbles of nodes disclose neighboring distance to solve any attack. The Route Setup Phase (RSP) is divided into four sub-phases:

   • Neighbor Propagation Phase: NPP
   • Loud Test Phase: LTP
   • Node Synchronization Phase: NSP
   • Level Propagation Phase: LPP

 

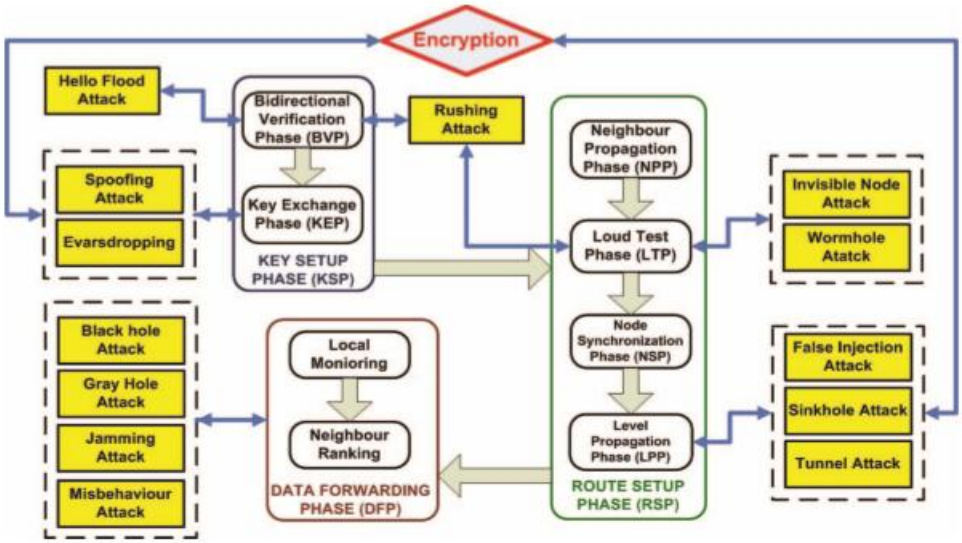


*Figure 4 Phases of RAEDD Protocol*

This paper mainly focusses on sinkhole attack, thus LPP [13] phase is used. In the RAEED technique time spams are used to assign levels to different nodes instead of traditional hop count increment message passing model. The base station starts LPP phase with broadcasting LEVEL messages contains generation time of message, next element of hash chain and Time encrypted using one way has chain. To solve problem of sinkhole on each node check the time span of the LEVEL message belongs. Then add remaining time in time span with delay to re-broadcast the LEVEL message. The time span is determined by consuming node level that have authentically assigned. The Time span is explained:

$$TS_N = T_B + (L_N * TL) \quad (1)$$

The error rate calculated with difference in time span and current time at nodes when message is recieeved. This error adds to any random time and rebroadcast the LEVEL message:

$$ST_N = (TS_N - CT_N) + (RT + TL) \quad (2)$$

**C. Data Forward Phase (DFP)**

IN DFP phase the Dave allows number of nodes are observed with the order of neighbors or local monitoring. A contract is based on order of data re-routing from the neighboring nodes in table. The aim of DFP is to resolve sinkhole, blackhole, jamming and other attacks.

## 2. AODV

AODV is a reactive routing protocol and determine routes only when needed. AODV used to discover the shortest and straight path during routing between source and destination node [14, 15]. In AODV the HELLO messages have used to notice and make connection between neighbors. Source node broadcast HELLO messages to all nodes and other nodes receive message. The disconnection is occurred between nodes if node reject HELLO message. When HELLO message sent to any unknown destination then the RREQ (Route Request) message sent to that location. When RREQ message received by any node that node became source for some time.

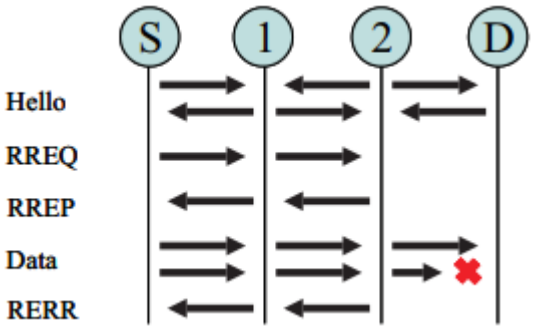


Fig. 5. Working of AODV Protocol

At intermediate node when RREQ is received a route is generated to source. If receiving node not receive RREQ rebroadcast it. When destination node reached then RREP (Route Reply) is generated. The RREP

 

propagates, each intermediate node creates a new route to destination. When source receives the RREP then it records the route and start sending data. If multiple RREP are received then it chooses the shortest hop count path. In unicast nature if node become source node while in multi case nature node become destination node. The Fig. 4. Explain all the steps of AODV protocol's working.

## V. Computer Simulation and Results

Computer simulations were performed using MATLAB [16] simulator to confirm the results and to test large networks. Moreover, real world effects like noise , collision etc can also be observed. Note that MATLAB can test up to 50 to 300 nodes and can measure throughput, message lost and Error rate during simulation. A total number of 15 to 20 experiments have been performed number of average neighbors was fixed to 24 and tests were performed both in presence and absence of noise. The results are calculated according to variation in number of nodes, variation in Density and Delay. Throughput is the total packets transferred during the whole simulation process. The Figure 5 shows the Throughput calculation with variation in number of nodes.

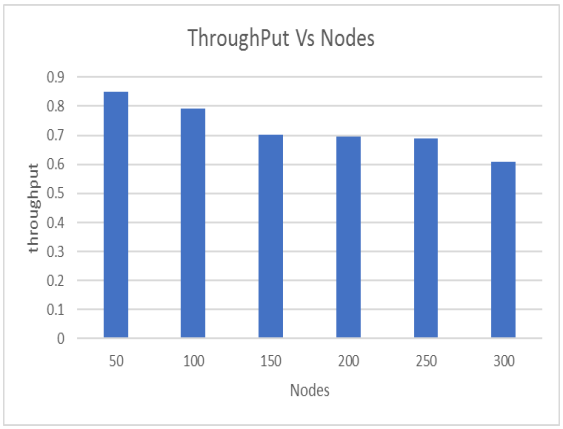


*Figure 6. Throughput VS Nodes*

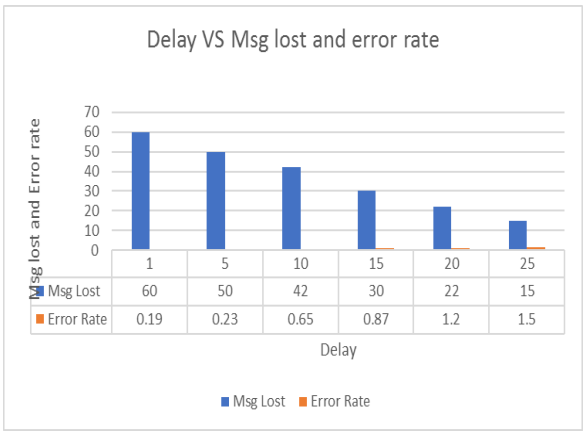


*Figure 7 Message Lost and Error rate VS Delay*

The Message Lost is referred to data lost during transmission of data from source to destination. Message lost is calculated by the difference of sender data and received data. In this proposed work message lost is calculated with variation in Delay, Time span and Density. The results of Message lost are shown in Fig. 6, Fig. 7 and Fig. 8. Same way the error rate is calculated.

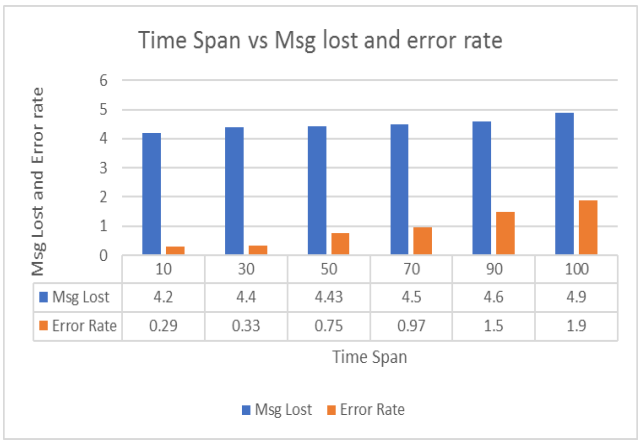


*Figure 8. Message Lost and Error rate VS Time Span*

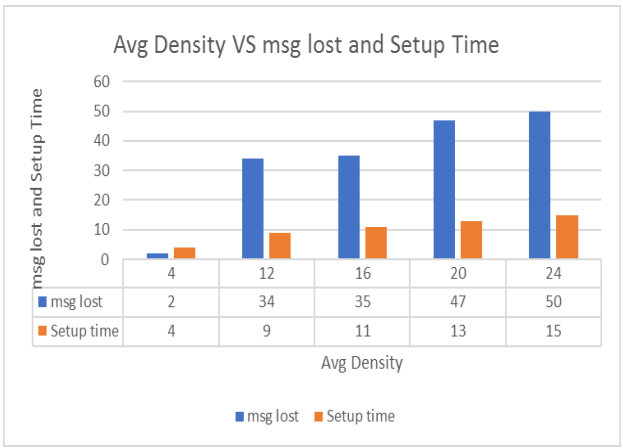


*Figure 9 Message Lost and Setup Time VS Density*

When the data is transferred from source to destination some data is lost. thus, the comparison is done on the basis of message lost with variation in Average Delay and Average Density. Delay is the time taken by any message to be send from source to destination and Density is the amount of information that is send during the data transmission. The values are enhanced during the simulation process of proposed work.

 

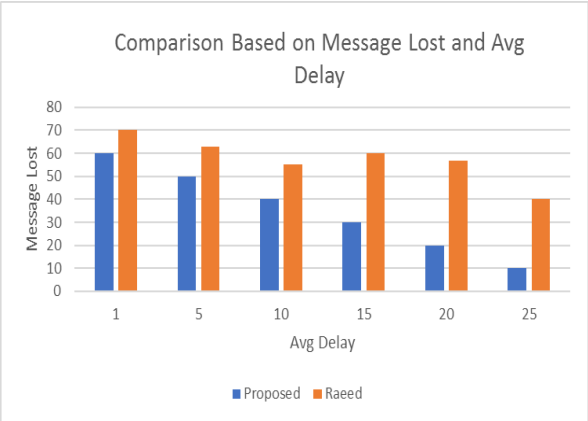


***Figure 10 Comparison Based on Message Lost and Average Delay***

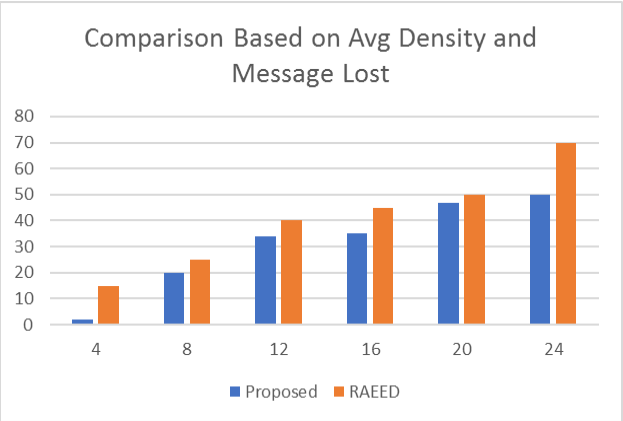


***Figure 11. Comparison Based on Message Lost and Average Density***

As shown in Figure 9. and Figure 10. The results are better as compare to RAEED protocol. The Message Lost rate is enhanced as compare to previous approach.

## VI. CONCLUSION

Our objective for this paper is to develop a system that control the sinkhole attacks in WSN environment. The Sinkhole attacks are occurred in route between source and destination of message delivery. The different protocols are used to control these attacks. In our Proposed work RAEED protocol and AODV protocol are hybrid. The features of both algorithms provide less error rate, less message lost and low setup time as compare to previous approaches. The ABC (Artificial Bee Colony) algorithm is used to find the route between source and destination. The comparison of Hybrid proposed approach RAEED and AODV with RAEED is considered and our proposed work gives better results than other two approaches. From the simulation results, this is concluded that removal of Sinkhole attack is achieved and parameters are better as compare to RAEED approach. In future, we plan to find better solutions to the problem of attacks by using improved protocols.

## REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, “An overview of Mobile Ad hoc Networks: Applications and challenges”, Sint Pietersnieuwstraat 41, Belgium, pp.50,2005.

[2] Nadeem, Adnan, and Michael Howarth. "Adaptive intrusion detection & prevention of denial of service attacks in MANETs." In *Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the world wirelessly*, pp. 926-930. ACM, 2009.

[3] Xing, Fei, and Wenye Wang. "Understanding dynamic denial of service attacks in mobile ad hoc networks." In *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pp. 1-7. IEEE, 2006.

[4] Gauri Kalnoor, Jayashree Agarkhed and Siddarama R. Patil “Agent-Based QoS Routing for Intrusion Detection of Sinkhole Attack in Clustered Wireless Sensor Networks" *Proceedings of the First International Conference on Computational Intelligence and Informatics*, Springer Science Business Media Singapore 2017 no. 12 (2016): 2343-2351.

[5] Gandhewar, Nisarg, and Rahila Patel. "Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network." In *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on*, pp. 714-718. IEEE, 2012.

[6] Kashif Saghar, Mamoona Tariq, David Kendall, Ahmed Bouridane “RAEED:AFormally Verified Solution to Resolve Sinkhole Attack in Wireless Sensor Network" *IBCAST, IEEE Transactions on* 28, no. 12 (2016): 2111-2124.

[7] Ehsan, Humaira, and Farrukh Aslam Khan. "Malicious AODV: implementation and analysis of routing attacks in MANETs." In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 1181-1187. IEEE, 2012.

[8] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. In Proc. Of the 13th European Wireless Conference.

[9] 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).

 

[10] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE

[11] Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE

[12] K. Saghar, W. Henderson, and D. Kendall. Formal modelling and analysis of routing protocol security in wireless sensor networks. In PGNET '09, pages 73–78, 2009.

[13] K. Saghar. Formal Modelling And Analysis Of Denial Of Services Attacks In Wireless Sensor Networks. Ph.d. dissertation, School of Computing, Engineering and Information Sciences, Northumbria University, Newcastle upon Tyne, UK, 2010.

[14] Harris Simaremare and Riri Fitri Sari, "Performance Evaluation of AODV variants on DDoS, Blackhole and Malicious Attacks", International Journal of Computer Science and Network Security, VoL-11, June 2o11, pp.6.

[15] Royer, Elizabeth M., and Charles E. Perkins. "An implementation study of the AODV routing protocol." In *Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE*, vol. 3, pp. 1003-1008. IEEE, 2000.

[16] Brown, Robert Grover, and Patrick YC Hwang. "Introduction to random signals and applied Kalman filtering: with MATLAB exercises and solutions." *Introduction to random signals and applied Kalman filtering: with MATLAB exercises and solutions, by Brown, Robert Grover.; Hwang, Patrick YC New York: Wiley, c1997*. (1997).

 