IDENTIFYING BLACKHOLE ATTACK IN WSN BY CHECK AGENT USING MULTIPLE BASE STATIONS

A.Anjaiah[#1] P.Tarakumari[#2] B.P.Soundarya[#3]
[#1,2,3]St.Peter's Engineering College, Telangana, India.

Abstract – **Due to the remote nature and foundation less condition of WSN, they are increasingly powerless against numerous kinds of security assaults. This paper proposes a procedure to recognize the dark gap assault utilizing numerous base-stations and a check specialist based innovation. This system is Energy proficient, Fast, Lightweight and Reduces message intricacy. A viable arrangement is recommended that utilizes various base stations to enhance the conveyance of the bundles from the sensor hubs coming to no less than one base station in the system, in this manner guaranteeing high parcel conveyance achievement. The proposed procedure is more proficient than the past strategies and gives better outcomes. Check specialist is a product program which is self-controlling and it moves from hub to hub and checks the nearness of dark opening hubs in the system. Steering through numerous base stations calculation is possibly enacted when there is an opportunity of dark gap assault on the system.**

Keyword: WSN, Black-hole assaults, different base stations and Check specialist.

I. INTRODUCTION

A WSN is made out of vast number of sensor hubs which are appropriated in the remote condition. This element permits an arbitrary conveyance of the hubs in the catastrophe alleviation activities or difficult to reach landscapes and a few different applications. Alternate applications [9] of WSN incorporates ecological control, for example, putting out fires or marine ground floor disintegration, additionally introducing sensors on extensions or structures to comprehend seismic tremor vibration designs, observation errands of numerous sorts like gatecrasher reconnaissance in premises, and so forth. Because of the remote nature and framework less condition of WSN, they are progressively helpless against numerous sorts of security assaults. By and large, the assaults are of two kinds in WSN-dynamic assaults and the aloof assaults. Dark gap assault is one of the hurtful dynamic assaults.

II. BLACK HOLE ATTACK

Dark gap assault In the dark gap assault, a malignant hub publicizes the wrong ways as great ways to the source hub amid the way discovering procedure as in responsive steering conventions or in the course refreshing messages as in proactive directing conventions. Great way implies the briefest way from source hub to the goal hub or the steadiest way through the sensor arrange. At the point when the source select the way including the aggressor hub, the traffic begins going through the foe hub and this hubs begins dropping the bundles specifically or in entirety. Here, these re-modified hubs are named as dark gap hubs and the locale containing the dark gap hubs are dark opening area. Dark gap locale is the section point to countless assaults [14].

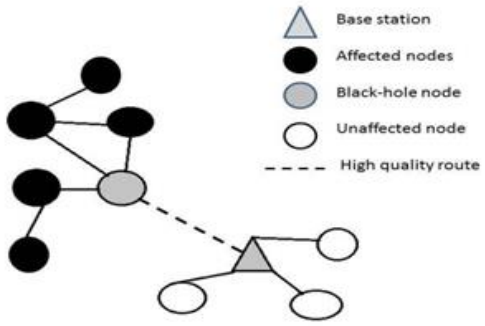

Fig 1: Black hole attack

III. CHECKING AGENTS & MULTIPLE BASE STATIONS

In a WSN, effective parcel conveyance to the BS is more basically required than the counteractive action of information to be caught by an aggressor. By utilizing productive information encryption calculations, for example, AES and information obscurity strategies, the data caught by an assailant can be made insignificant. In this way, spotlight ought to be on the goal of conveying the parcels to the BS within the sight of dark gap hubs. Here, a great arrangement is recommended that utilizes different BSs put in the system to enhance the conveyance of parcels from the SNs coming to somewhere around one BS in the system, in this way guaranteeing high bundle conveyance achievement. In a WSN, a BS is a PC class gadget so conveying numerous BSs is cheap. Here, numerous BSs are utilized to enhance information conveyance within the sight of dark opening assaults.

Check operator is a product program which is self-controlling and it moves from hub to hub and checks the nearness of dark gap hubs in the system. The system is actualized utilizing java dialect and the outcomes are contrasted and without the check specialists.

IV. Related Work

An Algorithm has been proposed in which the rundown of neighbouring hubs is kept up by every hub in the system. Steering way is built up here utilizing Dijkstra calculation. At first, directing is done through the closest base station i.e., without utilizing numerous base stations method. Directing through numerous base stations is possibly enacted when there is an opportunity of dark opening assault

in the system. It is required in the sensor systems to spare the vitality. Steps engaged with calculation are:
Stage 1-Routing through closest base station is initiated to send the parcels.
Stage 2-when there is an opportunity of dark gap assault at that point to check the nearness of dark gap hubs in the system, Check operator arbitrarily visits each hub in the system
Stage 3-When check specialist visits a hub
*Checks the recurrence of accepting bundles for each neighbouring hub in the rundown of hub „i".
*If it discovers 0 (No bundle from hub „j" to „i") for neighbouring hub „j",
*It questions hub „j" is a dark opening hub and it triggers directing procedure calculation through various base stations for time t.
Stage 4-Within time „t", it affirms whether hub „j" is a dark opening hub or not.

Parameters	Value
Network scale	200*200
No. of nodes	Random
No. of base stations	4
No. black-hole nodes	4
No. of check agent	1

Stage 5-If hub „j" is a dark opening hub, it disavows hub „j".
Stage 6-After time „t", it triggers steering process calculation through closest base station.(without utilizing different base stations).

V. Implementation Results

The technique is implemented using java language and the results are compared with and without the check agents. The parameters taken as shown below:

Parameters used

This technique proves 99% better results than the previous techniques. The detection of the black-hole by the check agent is done in a better way with 99% assured. The results are shown below.

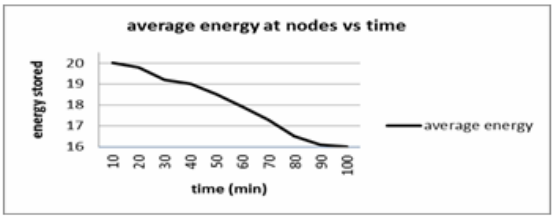

Fig. 2 Average Energy at nodes vs. Time

Fig. 3 shows that the no. of nodes increases as the radius of the black-hole region increases. As large is the black-hole region, more it covers the black-hole nodes.

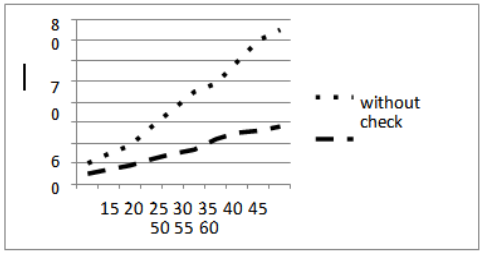

Fig. 3 shows the message complexity with no. of nodes with and without check agent.

It is shown that message complexity is more without check agent and less with the check agent

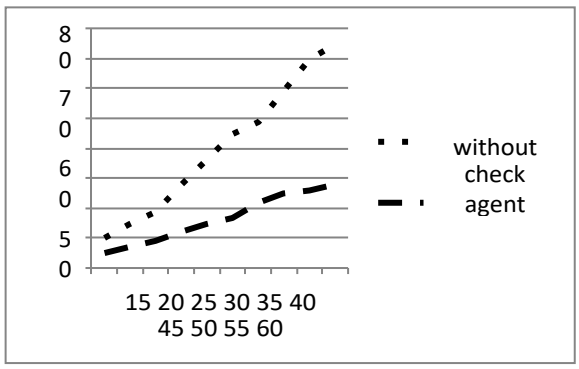

Fig 4 : Message complexity vs No .of Nodes

V. Conclusion

The proposed work demonstrates a 100% location procedure to keep the event of dark opening assault in WSN. This system utilizes steering through different base stations just when there is an opportunity of event of dark openings in the system. Generally steering through closest base station is done to decrease additional utilization of messages in the system. Subsequently, it lessens the utilization of vitality in the system by the hub which is a central point which is restricted and is to be considered cautiously in the sensor systems. Check operator assumes a noteworthy job in the discovery of dark openings in the system and furthermore lessens additional overhead from the system. The information conveyance is guaranteed as there is an arrangement of utilizing numerous base stations in the system. Be that as it may, the work should be possible further to deal with the message intricacy and to utilize less number of base stations in the system for better conveyance results in the remote sensor systems.

REFERENCES

[1] Zhu Miaoliang, Qiuyu. "Mobile Agent System" Journal of Computer Research and Development, vol. 38(1), 2001, pp. 16-25.
[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, 2002.
[3] L. Tong, Q. Zhao, S. Adireddy. "Sensor Networks with Mobile Agents", IEEE Military Communications Conference, Boston, MA, USA, 2003, pp.688-693;
[4] Zhang Yuyong, Jingde. "Mobile Agent Technology" Beijing, Tsinghua University Press, 2003;
[5] W. Lou, W. Liu, Y. Zhang, and Y. Fang. "SPREAD: Enhancing data confidentiality in mobile ad hoc networks"; In IEEE INFOCOM, volume 4, 2004. pp. 2404–2413;
[6] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks"; In ACM Workshop on Real-World Wireless Sensor Networks, 2005;
[7] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. "The Internet Motion Sensor: A distributed black-hole monitoring system", In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS), 2005; pp. 167–179;
[8] W. Lou and Y. Kwon. "H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks"; IEEE Transactions on Vehicular Technology, 55(4):1320–1330, 2006.
[9] R. Kompella, J. Yates, A. Greenberg, A. Snoeren, "Detection and Localization of network black holes"; In Proceedings of IEEE INFOCOM, 2007, pp. 2180–2188.
[10] S. Roy, S. Singh, S. Choudhary, and N. Debnath. "Countering sinkhole and black hole attacks on sensor

networks using dynamic trust management"; In IEEE Symposium on Computers and Communications, 2008; pp. 537–542.

[11] Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes" In IEEE INFOCOM, 2009. pp. 2846–2850.

[12] G. Sladic , M. Vidakovic and Z. Konjovic "Agent based system for network availability and vulnerability monitoring" 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics, September 8-10, 2011, Subotica, Serbia.

[13] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

[14] Atul Yadav et al., "Study of Network Layer Attacks and Countermeasures in Wireless Sensor Network" International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012.

[15] Gulshan Kumar, Mritunjay Rai and Gang-soo Lee "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement" International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012

[16] M. Ketel, N. Dogan, A. Homaifar. "Distributed Sensor Networks Based on Mobile Agents Paradigm" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) Singapore, 2012;

[17] Ping YI, Ting ZHU, Ning LIU, Yue WU, Jianhua LI "Cross-layer Detection for Black Hole Attack in Wireless Network" Journal of Computational Information Systems 8: 10 (2012) 4101-4109, 2012.