JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

Efficient Black Hole Attack Detection Mechanism for 6lowpan Wireless Networks

R.Sujatha[1*], P. Srivaramangai[2]

[1]Dept. of Computer Science, MaruduPandiyar College, Thanjavur , Tamilnadu,India
[2]Dept. of Computer Science, MaruduPandiyar College, Thanjavur , Tamilnadu,India

Available online at: www.ijcseonline.org

Abstract— In particular wireless networks, IPv6 Low Power over wireless personal area networks is a specific network configuration frame- work with the low power wireless devices with limited processing capabilities. In this network, the malicious node attacks over at the network layer. Moreover it is an unstable network, the formation of the path of networks only through the AODV Routing Protocol. In the view of security aspects the existing techniques were proposed in MANET but these are more vulnerable in 6LoWPAN Networks. It is increased number of packet dropping attacks like Black Hole attacks may cause the undesired operations in the time of routing the packet transfer. Thus the existing cryptographic systems are not sufficient to protect and very difficult and defend the routing protocol RPL. Here a new data aggregation based mechanism for black hole attack detection has been proposed in efficient manner. In this mechanism, the black hole node is detected by frequent monitoring and trustworthy prediction of reply packets that are transmitted by the sensor nodes and it will be removed from the network. The implementation results show that the improved efficiency in the detection of black hole attacks with MANET. More experiments were discussed about the detection mechanism in MANET.

Keywords- 6LoWPAN, Wireless Sensor Networks, Black Hole Attacks, Routing Protocol, AODV, Data Aggregation

I. INTRODUCTION

In trend emerging Internet of things, wireless sensor networks play a vital role in the trusted and confidential networks. In MANET, the black hole attacks make more trouble in the data communication between the mobile nodes. In existing, some of the techniques were proposed to detect the black hole attacks and isolate the network by taking the intensive countermeasures. Like MANET the mobile nodes or sensor nodes are connected together to form a network. Rather than the MANET, the 6LoWPAN Networks require the more concentration on the security issues because the anonymous users can also access to the mobile network through the edge router. Here, the proposed work incorporates the detection and mitigation of the black hole attacks in 6loWPAN Network.

That's the sensor nodes create smart network world where all the machines interact with each other automatically. The most vital role is to collect enormous amount of sensor data and the likelihood of the far-off control will be a most incredible benefit that will help many application domains. 6LoWPAN is an IETF-standardized IPv6 adaptation layer that enables IP connectivity over the loss , low power network links. It is used mostly in the Internet of Things applications including the industrial access control systems and smart cities. Special purpose upper layer protocols are used to IP based communicate in wide range of applications of 6LoWPAN networks.

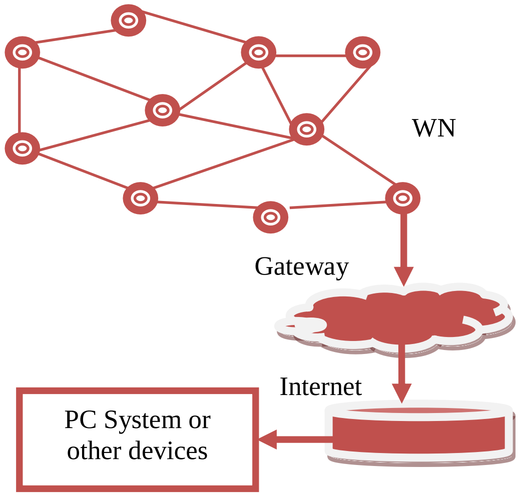

Fig. 1. Architecture of 6LoWPAN Networks

The Network Access control systems can be used to manage the number of sensor node s in the networks that is size of the networks, reliability of the nodes should be increasable and extending the node lifetime. Moreover, network admission control can also be used for the security. In this paper, we consider the problem of black hole attacks in the time of routing the packet transfer. Our solution follows the approach of network data aggregation by preventing the unauthorized nodes to communicate with the authorized nodes or to use the WSN to communicate with the Internet.

The main contributions of this paper are as follows. 1. The low power and low processing capability nodes are used to form a network called 6LoWPAN. 2. To create a mechanism for node clustering and cluster head identification using compressive sensing. 3. To propose a Intrusion Detection System with key management for black hole attack detection.

II. RELATED WORK

Anitta Vincent et.al. (2012) obtain the study of security aspects in 6LoWPAN with regards to its security threats and counteractions to address these issues. This paper studies the network framework with the regard to its security threats and counteracts to address the security issues. It deals with the cluster based key management schemes seem to be appropriate. This is done in order to obtain the signs of intrusion through digital key management.

R.Hummen et.al.(2013) provide a detailed security analysis of the 6LoWPAN fragmentation mechanism. They identified the major attacks by only sending a single protocol compliant network fragment. They proposed the lightweight defense mechanism using the content sharing scheme and split buffer approach.

A Rghioui et.al. (2014) focused on the denial of service attacks, they determined the intrusion detection system and provide solutions effectively and they concise the 6LoWPAN-RPL base networks. They protect the RPL from the internal attacks and undesired operations.

Karishma Chugh et.al. (2012) analyzed the harmfulness of malicious node attacks such as black hole attacks in the transport layer on 6LoWPAN-RPL. This work could strengthen the knowledge of various forms of attacks their effect on wireless sensor networks, parameters to facilitate identification of attack and attacking nodes and ultimately help the node will introduce a string defense system. Thus the variations in the parameters based on the harmfulness of the malicious node and its attacking feature.

Luuis M.L.Oliveira et.al.(2017) proposed solutions for the network admission control for 6LoWPAN as a wireless sensor networks that disallows the unauthorized nodes from using the network to communicate with the internet and the legitimate nodes in the networks. It avoids the collusion attacks in the clustered wireless sensor networks. They deals with the problem of neighbor discovery and routing protocols and also concentrates to reduce the number of control messages.

In order exploit the IOT environment and to promote the M2M communication applications, Yue Quie and Maode Ma (2017) proposed a mutual authentication scheme and key mechanism for avoid the black hole attacks and packet dropping attacks in the 6LoWPAN networks. The Protocol Composition Logic can provide the security .

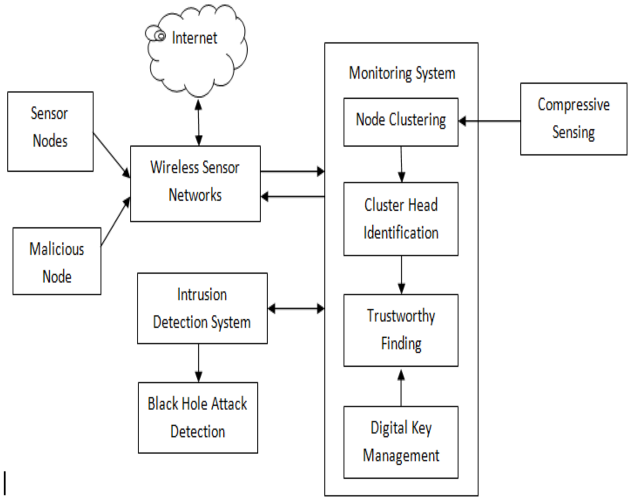

Fig 2 . Architecture of Proposed Work

III. PROPOSED WORK

A novel mechanism has been proposed with the intrusion detection system to detect the black hole attacks in wireless sensor networks. The sensor nodes are connected to form the wireless networks. Over the wireless networks, the devices connected with the internet through the gateway or router. The sensor nodes are clustered for data aggregation. In this cluster, the cluster head can be identified using compressive sensing algorithm. The data can be transferred through the cluster head after the trustworthy finding.

The digital key management can be established to maintain the unique key for the nodes in the networks. Thus the aggregator receives the packets from the nodes collected and connected as clustered nodes and transferred to the network through the gateway. In cluster based IDS nodes are arranged in the distracted manner and non-linear. The cluster heads have the tasks of (i) data filtering and data fusion, (ii) detection of intrusions in the networks but it analyze the cluster itself and (iii) confidentiality and secure management.

IV. IMPLEMENTATION RESULTS

Take experiments in the Network Simulation tool with the sensor nodes by TCL Language.

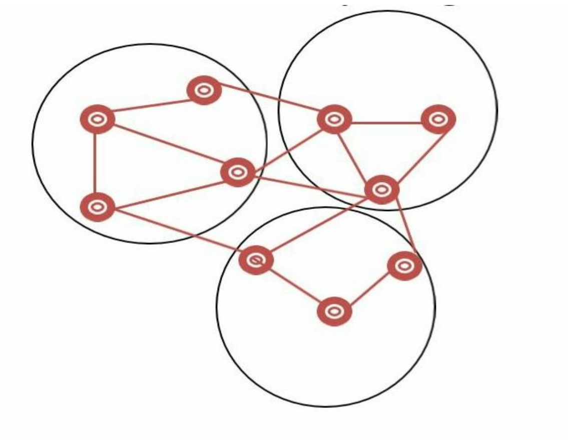

Fig 3. Cluster of Nodes

Algorithm for Clustering and Cluster Head Formation

Input: Cluster nodes and Optimal Cluster zie

Output: Clusters with Cluster Heads

```
Begin
        While(Ts has not expired) do
     If state = plain && has not sent              join_msg to the nearest cluster head
Else if state = head do
       Receive join_msg from its neighbor plain nodes
End
End
If state =head do
       Broadcast schedule_msg
End
End
```

Let us consider the node formation can be done by using experimental sensor nodes. The sensor nodes should be clustered by means of optimal cluster size. After the process of clustering, the cluster head or data aggregator node can be assigned by using compressive sensing algorithm. The implementation of the digital key management for the each and every sensor nodes in the network. The packet transfer has been enabled through the network clusters. Thus the cluster head performs the packet forwarding to the destination. The experimental nodes and the details of the node as follows:

S.No.	No. of nodes	Optimal Cluster Size	Black Hole Attackers
1	50	5	2
2	100	10	3

Thus the above node structure should be followed to obtain the node clustering and intrusion detection system.

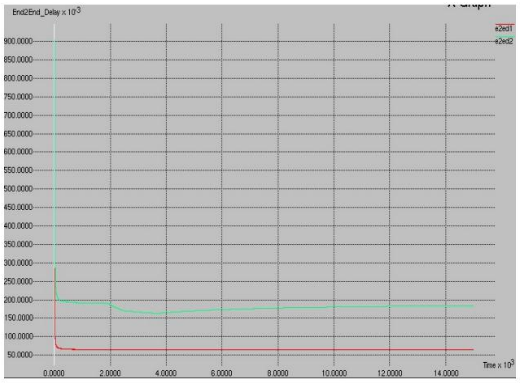

Fig 4. End to End Packet Delay

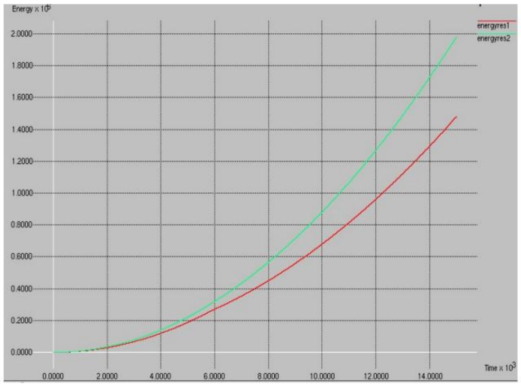

Fig 5. Energy Required

Thus the results show that the attack detection mechanism with the efficiency.

V. CONCLUSION

Thus the mechanism for intrusion detection system of black hole attacks proposed and experiment results have been also proved using simulation. In future, the jamming attacks and the denial of service attacks can be detected and resolved in the IPv6 over Low power Wireless Personal Area Networks.

References

[1] Chunnu L and A Shrivastava, "*An Energy Preserving Detection Mechanism for Black Hole Attack in Wireless Sensor Networks*", Intl. Journal of Computer Applications Vo.115, No.16, April 2015.

[2] D Nitnaware and A Thakur, "*Black Hole Attack Detection and Prevention Strategy in DYMO for MANET*", 3rd Intl., Conf. on Signale Processing and Integrated Networks",2016.

[3] B Singh, D Srikanth and C.R.S Kumar, "*Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective*", IEEE Intl. Conf. on Engineering and Technology, March 2016.

[4] O Shivwanshi, R Patel and P Saxena, *" Cluster Based Secure WSN against the Balckhole and Grayhole Attack*", Intl. Journal of Computer Science and Information Technologies, Vol.6, No.6, 2015, pp.5470-5472.

[5] Anitta Vincent, Fincy Francis and Ayyappadas P.S, "*Security Aspects in 6lowpan Networks*", IOSR Journal of Electronics and Communication Engineering, 2012.

[6] Kalaiselvan.K and Gurpreet Singh, "*Detection and Isolation of Black Hole Attacks in Wireless Sensor Networks*", International Journal of Innovative Research in Science, Engineering and Technology, Vol.4, No.5, May 2015.

[7] R Hummen, J Hiller, H Wirtz, M Henze, H Shafagh and K Wehrle, "*6LoWPAN Fragmentation Attacks and Mitigation Mechanisms*", Hungary, April, 2013.

[8] A Rghioui, A Khannous and M Bouhorma, "*Denial of server attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition*", Journal of Advanced Computer Science and Technology, Vol.3, No.2, pp.143-153, 2014.

[9] K Chugh, A Lasebae and J Loo, "*Case Study of a Black Hole Attack on 6LoWPAN-RPL*", Securware 2012: The 6th Intl. Conf. on Emerging Security Information, Systems and Technologies, UK, 2012.

[10] Luis M.L. Oliveria, Joel.J.P.C Rodrigues, Amaro F.Sousa and Victor M.Denisov, "*Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms*", IEEE Trans. on Industrial Informatics, Vol.12, No.6, December 2016.

[11] Yue Qie and Maode Ma, "*A Mutual Authenticaticaton and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks*", IEEE Trans. on Industrial Informatics, Vol.12, No.6, Decemeber 2016.

[12] F Ahmed and Young-Bae Ko, "*Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks*", Article in Research Gate, October 2016.

[13] J Deny, A Sivaneshkumar, M. Sundarajan and V.Khanna, "*Defensive against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach*", Intl. Conf. on Algorithms and Applications in Emerging Technologies, December 2017.

[14] R.Sujatha, Dr.P.Srivaramangai, "*Enhancing security in Manets Communication Issues and Mechanisms*", International Journal of Computer Techniques – Vol. 4 – Issues 3 (79 - 83) May – June 2017, ISSN: 2394–2231.

[15] R.Sujatha , Dr.P.Srivaramangai, "*A Survey on Network Layer Attack Detection And Isolation Techniques in Manet*" International Journal Of Modern Engineering Research (IJMER), vol. 07, no.12 , Dec - 2017, pp. 01 – 04.