A Review Approach on Detection and Mitigation Solutions of Network Layer Attacks

Khushboo Tripathi[1] and A. K. Malviya[2]
KNIT SULTANPUR

***Abstract*:** The rapid growth in the deployment of wireless networks attracts the attackers as a target. Network layer is vulnerable for different types of attacks like Sinkhole, Wormhole, Sybil, Selective Forwarding, Hello Flood, Black Hole, greyhole etc. Cooperative nature of nodes exposes sensor network to various kinds of passive and active attacks. The main focus of review is to sumup old and new techniques for detection and mitigation of network layer attacks and its consequences in different application areas.

Index Terms: *Security attacks, secure protocols, trust mechanism*

I. Introduction

The rapid growth of network deployment attracts different threats and attacks in the network. However researchers are greedy to search the solution of detection of those attacks and prevention from them for the benefit of society. Various attacks were detected and many solutions are proposed but still research is needed to find out the more solutions for mitigation from attacks. A general description of existing attacks at network layer is given under the sections where different attacks and mitigation approaches have discussed. This review focuses on pre existing, current and future aspect of work. Many authors have given their idea to detect and prevent attacks in networks. Few of them are notified for the review work under the section 2.

Many security levels are defined for prevention in different ways. Some researchers focus on secure routing protocols while others have proposed new techniques in the network for mitigation. There are two major approaches: (i) making existing routing protocols secure (ii) proposing new namely secure routing protocol.

On the other side of invention and analysis, research is brought into highlights of new proposed techniques or algorithm for mitigation of attacks in the networks. Thus the below sections are illustrated a review work on these existing and proposed schemes.

II. Review of work

Many authors have given their ideas on detection and prevention techniques from attacks at network layer. Every approach is quite different with respect to scenario and assumptions. There are many solutions at network layer which are reviewed as below:

D.B. Patel, D. A. Patel [1], has presented the idea about " Trust Based Solution for Detection of Network Layer Attacks in Sensor Networks" .The authors have proposed the trust based mechanism for detection of wormhole attack that is already simulated for black hole attack. Simulation results are used with the NS-2 simulator and attack has been evaluated in term of packet delivery ratio, throughput, delay and routing overhead compare to a network without or with attack.

M. A. C. Aung and K. P. Thant [2] has given the solution for Detection and Mitigation of Wireless Link Layer Attacks". Wireless Link Layer Attacks Detection algorithm (WLLADA) is proposed by using active and passive finger printing methods to detect masquerading denial of service (DoS) attacks. Proposed algorithm is implemented with a real time set-up using in Kali linux environment with python network programming.

C. Ioannou and V. Vassiliou [3] has presented in their paper, "The Impact of Network Layer Attacks in Wireless Sensor Networks". In this work authors dealt with the detection phase and examined the impact of routing layer attacks in WSNs as an effort to build better intrusion detection systems (IDS). IDSs base their detection decision on the knowledge gained

from known attacks. Also they have implemented routing-layer packet drop attacks and investigated the impact of the attacks as "seen" from the Sink node and the victim node. The degree of impact depends on many factors, including the topology of WSN and the distance from the Sink.

Y. Najaflou, etal. [4], has expressed the new idea as "Safety Challenges and Solutions in Mobile Social Networks". This work narrowed the safety challenges and solution techniques down from OppNets and delay-tolerant networks to MSNs with the hope of covering all the work proposed around security, privacy, and trust in MSNs. To conclude, several major open research issues are discussed, and future research directions are outlined.

Qiuwei Yang, etal. [5], has presented a "Survey of Security Technologies on Wireless Sensor Networks". This paper summarized research progress of sensor network security issues as three aspects, key management, authentication, and secure routing, analyzed and commented on these results advantages and disadvantages and pointed out the future direction of the hot research field.

C. Liang and F. R. Yu[6], "Wireless Network Virtualization: A Survey, Some Research Issues and Challenges". The author indentifies several important aspects of wireless network virtualization: overview, motivations, framework, performance metrics, enabling technologies, and challenges. Finally, we explore some broader perspectives in realizing wireless network virtualization.

K. Tunwal, P. S. dabi, P. Sharma [7] has presented "An individual trust management technique for mitigating sinkhole attack in manet". The authors have given a new trust management technique for prevention from attack. The proposed algorithm was simulated using network simulator NS2 and the results showed that the proposed algorithm greatly reduces the sink-hole impact and performs much better than previous algorithm

H. M. Choi, etal. [8] has given the idea of "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks". The authors have proposed a secure routing method for detecting false report injections and wormhole attacks in wireless sensor networks. The proposed method used ACK messages for detecting wormholes and based on a statistical en-route filtering (SEF) scheme for detecting false reports. Simulation results showed that the proposed method reduces energy consumption by up to 20% and provide greater network security.

W. Shim, G. Kim and S. Kim [9], has written in their paper "A distributed sinkhole detection method using cluster analysis". The new approach was given in this paper by the authors i.e. clustering analysis in network.

S. Gisdakis, V. Manolopoulos, etal. [10], "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems". Authors have provided a full-blow n implementation on actual smart phones, along with an extensive assessment of its accuracy and efficiency. The results confirmed that smartphone-based TISs can offer accurate traffic state estimation while being secure and privacy preserving.

U.S.R.K.Dhamodharan, and R.Vayanaperumal [11], has given method for "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method. This paper deals with one of the hazardous security threats known as Sybil attack and proposes an algorithm known as message authentication and passing method to hinder a Sybil attack in a wireless sensor network. The work explains the message authentication and passing method is applied for checking the trustworthiness or otherwise for a Sybil node. The action of a node as a Sybil node with duplicate ID and in formation can happen only when the node has complete information about other nodes

N. Balachandaran and S. Sanyal [12], "A review of techniques to mitigate sybil attacks.

R. Amuthavalli and R. S. Bhuvaneswaran [13], authors have proposed new method for detection and prevention of sybil attack in wireless sensor network employing random password comparison method.

Chen, Honglong, et al.[14], again a new approach given in this paper about securing DV-Hop localization against wormhole attacks in wireless sensor networks.

Biswas, Santosh, etal. [15] has given trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET.

Taylor, Vincent F., and Daniel T. Fokum [16], a new idea given by author for mitigating black hole attacks in wireless sensor networks using node-resident expert systems.

Athmani, Samir, etal. [17] , authors have tried to explore in different aspects about hierarchical energy efficient intrusion detection system for black hole attacks in WSNs.

Wazid, etal [18], have proposed TBESP algorithm for wireless sensor network under blackhole attack.
Bin, Tian, et al.[19], in this paper authors had given a ranging based scheme for detecting the wormhole attack in wireless sensor networks.
G. Otero, etal. [20] have explained secure neighbor discovery in wireless sensor networks using range-free localization techniques.
S.Raza,etal. [21] a new concept is given by author i.e. Svelte: Real-time intrusion detection in the internet of things. IoT is latest area where networks issue can be taken as challenge.
T. Giannetso, etal. [22], has explained thoughts about trustworthy people centric sensing Privacy, security and user incentives road-map.
S. Gisdakis, etal. [23], authors have given a new idea of research by paper SPPEAR: Security & Privacy-preserving Architecture for Participatory-sensing Applications.
J. A. Chaudhry, etal. [24] authors have highlighted in their paper sinkhole vulnerabilities in wireless sensor networks.
These above mentioned papers are totally focused on attacks and solutions to protect from them. These are few which are reviewed many other work has done in this area for fruitful options ahead.

III. Transform of review work

The new technology occurs and new approaches with research but actually the transform of review work still deals with the combination of old and new strategies. A good research is to investigate and analyze the thoughts of work. For review of detection and prevention of attacks the basic idea is as given in fig 1.

Review can be transformed
Look into Streams
Generalize the things
Study existing approaches
Modify/Explore new method/techniques/algorithms
Conclude: Idea to be proposed

Figure 1: Depicts Review Framework

The figure content is self-explanatory only the next step is to where is it applicable for detection and mitigation and how for the new researchers they can find the somehow the answer in in figure 2 and figure 3 as below. The latest research is going through different area of networks for attack cause.
There are few applications wherein attack can be implemented and analysed in different platforms like ns, opnet, omnet etc [25]. In manet's and sensor's attacks have implemented and anlysed but stil the research is open for the mitigation solution in other application areas like hybrid, vehcular and opportunistic networks.
Network Applications where attacks can be checked:

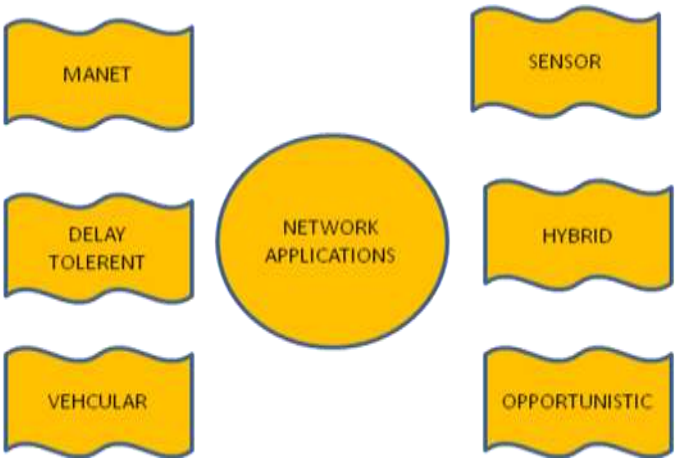

Figure 2: Research in Network Applications

In below figure 3, mitigation solutions are sumup which is briefly explained. After a deep study of research review for mitigation from attack at network layer, many solutions are found to improve the performance of network and data sharing. Some recent approaches are listed below:

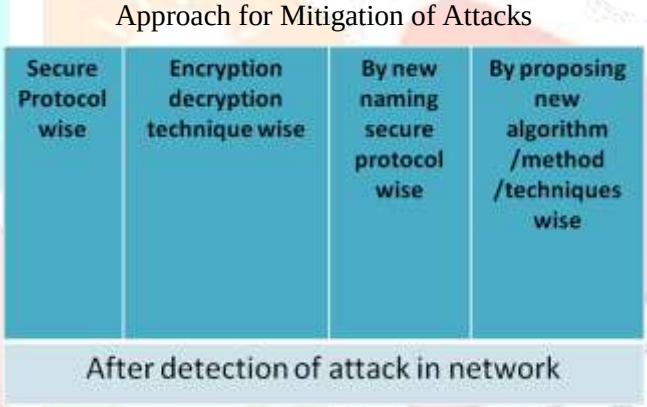

Figure 3: Mitigation solutions in Networks

a) Routing algorithm is the basis of information transmission and convergence in the wireless networks. Many secure routing protocols are proposed keeping in mind that no alteration in the assumptions in networks while attacks occur. In order to mitigate malicious behavior, secure routing secures the originality of nodes behavior in networks. The existing protocol with privacy preserving specific task is tuned into secure routing algorithm. This helps in mitigation solution from unknown and known attacks.

b) Encryption and decryption is another method to resolve the security issue in network. Some key management protocols with secure mechanism also works from malicious activity. Hashing technique including routing algorithm is also a way to protect information in the networks.

c) Some authors and community has proposed new naming secure algorithm for attack prevention. SRP (Secure Routing Protocol);ARIADNE :Ariadne is a robust protocol based on Dynamic Source Routing that has been proposed by Hu et al.; ARAN (Authenticated routing in ad hoc network);SEAD (Security aware ad hoc routing)

d) The new approach of mitigation of attacks has dealt with latest proposed schemes like trust mechanism, cluster analysis, range based scheme and security privacy based architecture scheme etc [1,7,9,19,23].

Thus its very hard to crack the decisions of numbers of results with these solutions. Some other way can be possible for detection prevention in future.

IV. Conclusion

Research on attacks in wireless networks is quite broad and a number of solutions for mitigation from attacks are notified. Nevertheless, it is in favor of the wireless community to address the issues to detect and prevent the challenges of attacks at network layer. This article attempts to briefly explore the current methods related to wireless network attacks and future research that may be beneficial in pursing the vision.

References

[1] D.B. Patel and D. A. Patel, "A Trust Based Solution for Detection of Network Layer Attacks in Sensor Networks", 2016 International Conference on Micro-Electronics and Telecommunication Engineering, IEEE, pp.121-126, 2016.

[2] M. A. C. Aung and K. P. Thant , "Detection and Mitigation of Wireless Link Layer Attacks", SERA 2017, June 7-9, London, UK, IEEE, pp.173-178, 2017.

[3] C. Ioannou and V. Vassiliou, "The Impact of Network Layer Attacks in Wireless Sensor Networks", 2016 International Workshop on Secure Internet of Things, IEEE, pp.20-28, 2016.

[4] Y. Najaflou, B. Jedari, F. Xia, L.T. Yang, and S. Mohammad, "Safety Challenges and Solutions in Mobile Social Networks", IEEE Systems Journal, Vol. 9, No. 3, pp. 1-21, September 2015.

[5] Qiuwei Yang, Xiaogang Zhu, Hongjuan Fu and XiqiangChe,"Survey of Security Technologies on Wireless Sensor Networks", Hindawi, Journal of Sensors, pp. 1-9, 2015.

[6] C. Liang and F. R. Yu, "Wireless Network Virtualization: A Survey, Some Research Issues and Challenges", IEEE Communication Surveys & Tutorials, vol. 17, no. 1, pp.1-24, 2015.

[7] K. Tunwal, P. S. dabi, P. Sharma, "An individual trust management technique for mitigating sinkhole attack in manet", International journal of computer application, volume 95-No.24,pp.39-43, 2014.

[8] H. M. Choi, S. M. Nam and T. H. Cho, "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks", Wireless Sensor Network, 5, pp.33-40, 2013.

[9] W. Shim, G. Kim and S. Kim, "A distributed sinkhole detection method using cluster analysis", Elsevier, 37,pp. 8486-8491, 2010.

[10] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems", IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 3, pp.1428-1438, 2015.

[11] U.S.R.K.Dhamodharan, and R.Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", The Scientific World Journal, pp.1-7, 2015.

[12] N. Balachandaran and S. Sanyal, "A review of techniques to mitigate sybil attacks,"
International Journal of Advanced NetworkingandApplications,vol.4, pp.1–6,2012.

[13]R. Amuthavalli and R. S. Bhuvaneswaran, "Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method," Journal of Theoretical and Applied Information Technologygy, vol. 67, pp. 236–246, 2013.

[14] Chen, Honglong, et al. "Securing DV-Hop localization against wormhole attacks in wireless sensor networks." Pervasive and Mobile Computing 16 (2015): 22-35.

[15] Biswas, Santosh, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." Applications and Innovations in Mobile Computing (AIMoC), 2014. IEEE, 2014.

[16] Taylor, Vincent F., and Daniel T. Fokum. "Mitigating black hole attacks in wireless sensor networks using node-resident expert systems." Wireless Telecommunications Symposium (WTS), 2014. IEEE, 2014

[17] Athmani, Samir, D. E. Boubiche, and A.Bilami. "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs." Computer and Information Technology (WCCIT), 2013 World Congress on. IEEE, 2013.

[18] Wazid, Mohammad, Avita Katal, and R. H. Goudar. "TBESP algorithm for wireless sensor network under blackhole attack." Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE, 2013.

[19] Bin, Tian, et al. "A ranging based scheme for detecting the wormhole attack in wireless sensor networks." The Journal of China Universities of Posts and Telecommunications 19 (2012): 6-10. [20] G. Otero, Mariano, and A. P. Hernández. "Secure neighbor discovery in wireless sensor networks using range-free localization techniques." International Journal of Distributed Sensor Networks 2012 .

[21] S.Raza,L.Wallgren,and T.Voigt,"Svelte: Real-time intrusion detection in the internet of things," Ad hoc networks, vol. 11, no. 8, pp. 2661– 2674, 2013.

[22] T. Giannetsos, S. Gisdakis, and P. Papadimitratos, "Trustworthy people centric sensing: Privacy, security and user incentives road-map," in Proc. Med-hoc-Net, 2014, pp. 39–46.

[23] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security & Privacy-preserving Architecture for Participatory-sensing Applications," in Proc. ACM WiSec, Oxford, U.K., 2014, pp. 39–50.

[24] J. A. Chaudhry, U. Tariq, M. A. Amin and R. G. Rittenhouse "Sinkhole Vulnerabilities in Wireless Sensor Networks", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.

[25] www.isi.edu/nsnam/ns/tutorial Marc Greis tutorial on ns2/ns3.