ADSMS: ANOMALY DETECTION SCHEME FOR MITIGATING SINK HOLE ATTACK IN WIRELESS SENSOR NETWORK

N. Mohammaed Yasin	N. Balaji	G. Sambasivam	M. S. Saleem Basha	P. Sujatha
Research Scholar, Department of Computer Science	Department of Computer Science and Engineering,	Department of Computer Science and Engineering	Department of Computer Science	Department of Computer Science
Pondicherry University	Sri Venkateshwaraa College of Engineering & Technology	KL University	Mazoon University College	Pondicherry University
India	India	India	Sultanate of Oman.	India
yascrescent@ gmail.com	nbalajimet1983@ gmail.com	gsambu@ gmail.com	m.s.saleembasha@ gmail.com	spothula@ gmail.com

Abstract*—In past years, mobile ad hoc networks (MANETs) widespread use in many applications, including for some mission-critical applications, and has become one of the major concerns such as security MANETs. MANETs due to some unique characteristics, prevention methods are not alone enough to protect them need; Therefore, the detection is possible for an attacker to breach system security, such as the need to add another before. In general, traditional wireless networks, intrusion detection techniques are not well suited for MANETs. In this case, to protect it from attacks MANETs is important to develop more efficient methods of intrusion detection. With improvements in technology and cutting hardware costs, we MANETs expanding into industrial applications are also witnessing a current trend. To cope with such a trend and we believe strongly that it was important for its potential security issues. In this paper, we propose new intrusion detection and specially designed MANETs Improved Acceptance acknowledgment (EAACK) to activate the digital signature system. Compared to contemporary approaches, while not greatly affect network shows EAACK certain conditions demonstrates the high detection rates of malicious behaviour...

Keyword-Wireless Sensor Network, Mobile Ad Hoc Network

I. INTRODUCTION

Manipulation replay attacks and denial of service that can cause serious consequences. Shortly, critical sensor data must be protected just as critical traditional network data, by preserving their confidentiality, integrity, authentication, and availability and freshness principles.

This paper work has mainly two objectives. The first is to provide a general understanding of Wireless Sensor Networks architecture. WSNs architecture needs to be studied, to obtain a basic understanding of how these devices are designed and work and how their power, computational and communication limitations determine the performance of the whole network. The second objective is to examine A Wireless Sensor Network (WSN) is defined as a large set of tiny sensor nodes (the number varies from few to several hundreds or thousands) with sensing, computational and communication capabilities. Already more advanced technologies, the origin of

978-1-5090-4797-0/17 $31.00 © 2017 IEEE
DOI 10.1109/ICTACC.2017.47

WSNs is founded in heavy industries and military apps. The Sound Surveillance System (SOSUS)[1], developed by the US Military in the 1950s, during the Cold War, to track and detect Soviet submarine, is the founder of modern WSNs. Later, in the early 1980s, the US Defence Advanced Research Projects Agency (DARPA) announced the Distributed Sensor Networks (DSN) program to investigate the benefits in invoking distributed wireless sensor networks, which was followed by the SensIT [2] program that provides the current sensor networks with new possibilities, such as dynamic querying, ad hoc networking, and tasking, multi-tasking and reprogramming. Subsequently, universities and governments had begun using WSNs in apps like forest fire detection, air quality monitoring, power distribution, natural disaster prevention, factory automation, , waste treatment and weather stations. At this time, all of the above military, science / tech and industrial apps were based on large, costly sensors with limited functionality, performance and scalability.

Major advances in micro electro mechanical systems (MEMS), CMOS-based semiconductor devices, networking protocols (IEEE 802.15.4 standard [3] or Zombie)and energy storage technologies, dramatically reduced the high deployment and mainly maintenance cost and leveraged the wide range of acquiring of WSNs into broader range of apps, including home automation, smart environments, continuous medical monitoring systems, environmental control and many others. In short, we can presume that future WSNs will be the part of the internet [4] (Fig. 1), changing our everyday life in unprecedented and unanticipated ways.

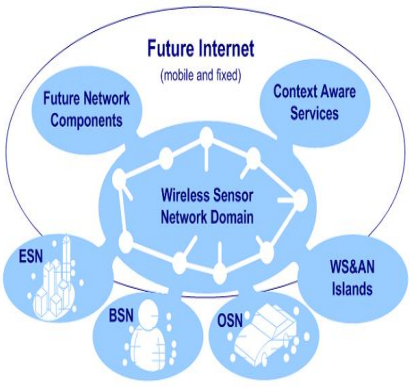

Fig 1.1 Future Internets

Since Wireless Sensor Networks can be used in various critical applications as stated, the data being transmitted must be secured to prevent security issues such as eavesdropping, data thoroughly the security issues that sensor networks have to confront, with respect to their limitations. The first limitation is the wireless transmission that can be eavesdropped by anyone. The second limitation is the lack of a permanent power source, which means that the security algorithm must be very efficient, but lightweight, so as to restrain energy consumption.

II. LITERATURE REVIEW

WSNs sinkhole which has been identified as one of the serious threats of attacks.In this type of attack, a malicious node is often used to advertise itself to its neighbors, and it was best path to a base-station. Due to malicious node network security and data is also likely to damage or tamper with normal operation…

The protocol used (Rajneesh Kumar, 2015) is Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. This uses its routing operation to detect the intruder in the network an IDS mechanism. In the proposed algorithm, the detection metrics, such as the no. of packets send and received are used to calculate the Intrusion Ratio (IR) by the Intrusion Detection System agent, based on the calculated numeric or non- numeric value in turn denotes the normal or malicious activity. The IDS system detects the sinkhole attack by the IR then the IDS agent alerts the network about the intruder node. The data transmission is not continued through the sinkhole node.

ETARF (Pushcart A. Cavan et al., 2015), a robust trust aware routing for WSNs against intruders in multi hop routing. This approach does not use any time synchronization or known geographic information to find the route from source to destination. Instead, it finds the shortest efficient route using the SPA(shortest path algorithm). This algorithm directs the logical link on the physical path with least hop count. The results shows that energy savings and bandwidth through clusters and data aggregation.

An approach (Leovigildo Sánchez-Casado et al., 2015) to detect sinkhole attack in MANETs with AODV routing. It focuses on the infected borders created by legitimate nodes under the guidance of intruders. The information collected form neighbour nodes at regular intervals are used to find the sink holes.

A novel approach (Fang - Jiao Hangar, 2014) for detecting serious security problems like sinkhole attack using redundancy mechanism. Multi paths are used for sending the messages. After evaluation of the replies the attacker nodes are identified. The simulation results show the effectiveness of this approach.

There are two approaches (Shadier, 2014) to identify and prevent sinkhole attacks. A common approach in turn detects attack in the infected regions in the network. A Geostatistical hazard model is used in this approach. The second approach, via distributed monitoring detects a malicious approach to analyze every neighbourhood in the network.

A Secure Energy Efficient Adhoc Routing Security (Rajang B. Patti and Dhanashree Kulkarni, 2014), is obtained through shared cryptography. A minimum Hop Routing is used for routing. Opportunistic algorithm provides multiple paths from source to destination. Information which has to be communicated is divided into multiple shares. The information is sent from source to destination through the multiple paths. Security is maintained through application of a secret sharing algorithm at source. The result of the simulation shows energy efficiency in terms of cost of security in warm hole, sinkhole attacks.

The simulation study (Fabric Le Fess ant et al., 2012) using a set of parameters like position, network scale and the number of infected nodes and impact of the different attacks. The study presents, a detailed metrics on malicious attacks. They have proposed a novel design of two simple and resilient protocols to apology based reconfiguration.

An IDS (Ioanniskrontiris, 2008) for Wireless sensor networks that can detect sinkhole attacks. The study in the approach explains how sinkhole attacks can be launched in realistic networks. This method uses the Min Route protocol of Tinos. The concept behind Misroute is use of the link quality metric to construct the routing tree. Rules are applied for identification of the intruder node with IDS system. The simulations results obtained in their approach shows the accuracy of the algorithm.

A sinkhole attack (Kim, 2007) that attempts to heavy network traffic to single sinkhole node in MANET. This approach focuses on the DSR protocol in MANET. Sinkhole indicators analyse the sinkhole problem and detect the sinkhole node. The intrusion detection algorithm used is incremental learning algorithm. The simulation results obtained show the effectiveness and reliability in detection of intrusion detection of sink hole.

III. System Design

A. Existing System

The main motive of the sinkhole attack, is to fake all the nearly traffic from a particular area through a settled node, by creating a denotative sinkhole with the attacker at the centre. Sinkhole attacks commonly work by making a compromised node looks specially more attractive to neighbour nodes with respect to the routing algorithm. Verifying sinkhole is difficult because we can't find which information is supplied by the node. As an example, a laptop-class adversary has a capability to transmit enough power to reach a WAN by radio transmitter. As shown in fig. 2 a infected node convince all the traffic as it was the shortest route to acquire the base station.

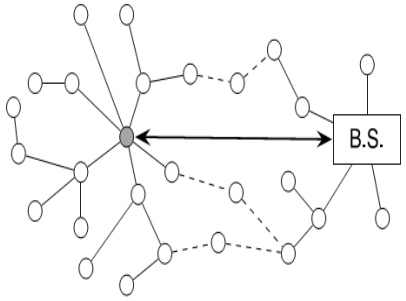

Fig 3.1 Example of sink hole attack. shaded node (sink hole) delivers packet to the base station (BS)

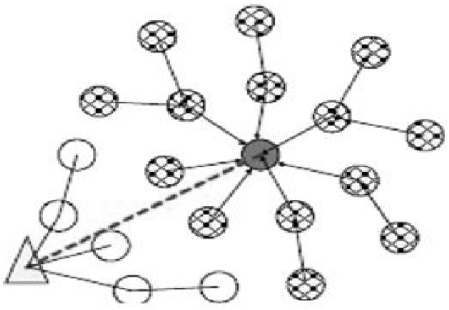

Fig 3.2 Sinkhole Using An Artificial High Quality Route

In the existing method, they are provided two different methods such as *Geostatistical detection method* and *Distributed detection approach.* Even though these method detects the sink hole node attack in the network. But lags in dynamic change network structure, for example when a source and destination communicates packets through hop nodes. There hop node may act as the sink hole attack node.

B. Proposed System

In this work, we propose a new monitoring scheme named Hop Count Monitoring Scheme. This scheme helps to identify the sinkhole attack with in the hop nodes. A sinkhole will be detected by the novel intrusion detection system. The schema is based upon hop count observing. Since the hop-count feature is obtained easily from routing tables, the ADS (Anomaly Detection Scheme) are easily implemented by a small footprint. Moreover, the proposed ADS will detect attacks with 96% accuracy and applicable to all rounting protocol that maintains dynamically a hop-count parameter.

IV. System Implementation and Results

The stimulation tool used in this project is Network Stimulator 2.It was chosen because of its wide range of features. The best feature provided by the network stimulator was open source code that can be modified

or extended. The latest version of network stimulator is ns-2.1b9a

B. **Mobile Networking In NS2.33**

NS2 in the slot to the CMU wireless model that was adopted by the Monarch group describes as an extension of the movement. The first section of the CMU / Monarch group mobility model ported from the original covers. In this section, we would be used to build a mobile node to a mobile node within the network stack, which includes a routing mechanisms and network components. Elements that are covered briefly channel, network interface, radio propagation model, MAC, protocol, interface queue, and address resolution protocol link layer model (ARP), are available. CMU trace Files node movement and traffic situation in this area in support and generation. Original CMU Pure model allows simulation of wireless LANs or multi-hop ad-hoc networks. These enhancements allow simulation model combined wired and wireless networks. The wireless model can be extended to mobile IP.

C. **The Basic Wireless Model In NS**

The wireless model has an additional supporting feature and essential feature of mobile node at the core that's allowing stimulation of multi-hop ad-hoc networks, LAN's. The mobile node has a capability of splitting its objects. Basic mobile node has additional functionality and the ability to move in the topology, capability to receive and transmit signals from a wireless channel etc...

D. **Simulation Results**

The simulation result has been performed with the help of the performance metrics such as PDR, beacon overhead and energy consumption. The PDR is calculated based on the no. of packets received by the target and the no. of packets generated by the origin.

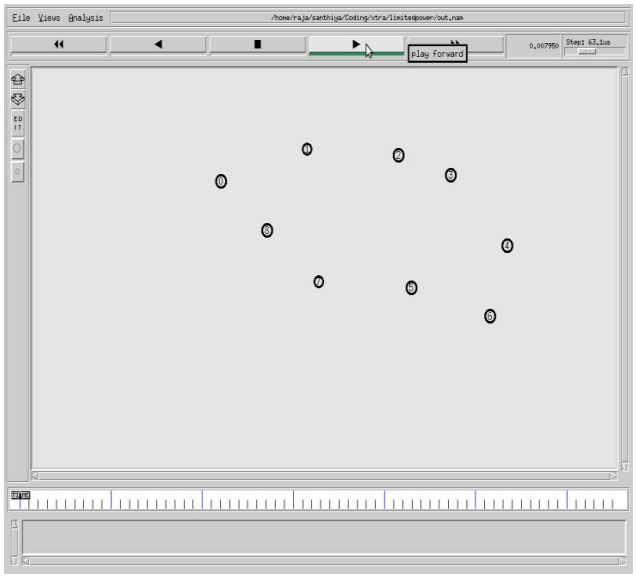

Fig 4.1 To searching the nodes

The below window is used to search the nodes from the avliable set of the node.

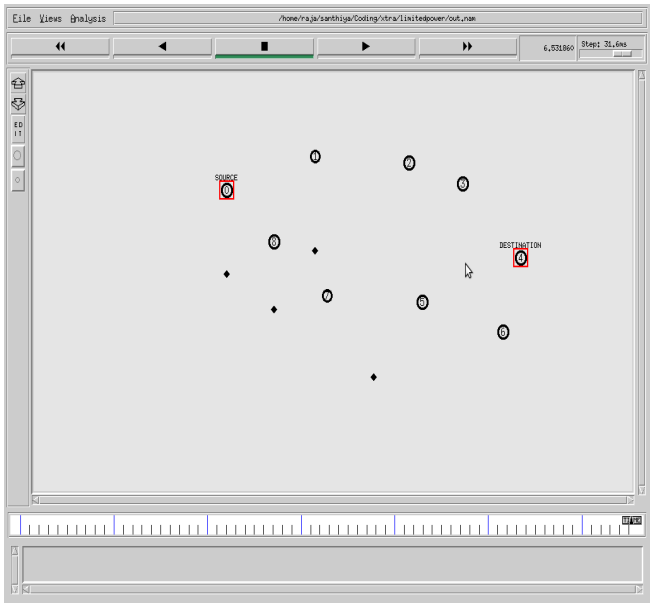

Fig 4.2 To find the energy nodes

The below window is usd to find the energy and unenergy nodes by using the colored node and to the red nodes are energy nodes as for the black nodes are unenergy nodes.

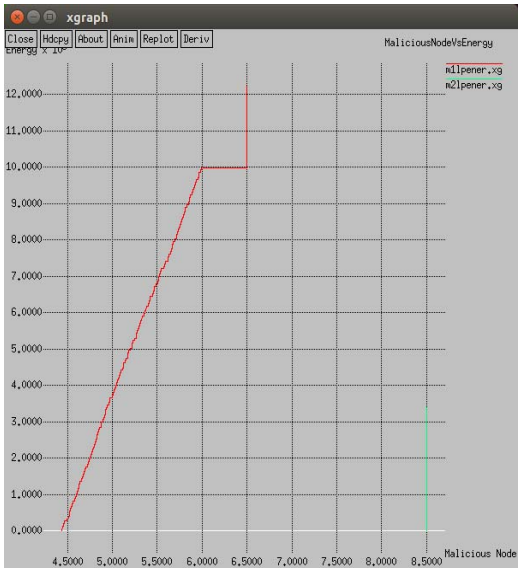

Fig 4.3 Graph (Existing Energy levels)

The above graph represented by the energy levels.

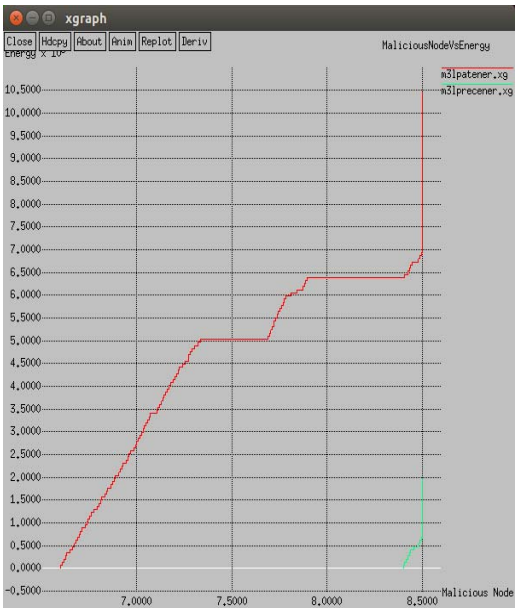

Fig 4.4 Graph (Proposed Energy levels)

The above graph as to represent the enegy proposed at the each stages and that haveto allocate the time based operation.

D. Performance Metrics

1) Packet Delivery Ratio: Packet delivery ratio (PDR) is defined as the ratio of data packets collected by the target to those developed by the origin. The performance metric for our protocol using different speeds for different traffic models based on the packet distribution functions gives an idea of how well the protocol is performing. Mathematically, is defined as,

$$PDR(\%) = \frac{\sum_{I=1}^{M} Sum\ of\ data\ packets\ recived\ by\ each\ destination}{M}$$

(4.1)

Where, i, indicates the no. of O/P file

M, indicates total no. of O/P files

2) Energy consumption: Energy consumption is calculated as the difference between initial energy and the amount of energy required for routing process.

V. Conclusion And Future Enhancements

A. Conclusion

This effective method shows how to oppose both the attacks on WSN. In the overhead sections, we proposed novel ideas based on DDMS to deal both the attack separately. These attacks are consecutive but not combining so we should handle the attacks separately. It can support multiple severe attacks by the considerable stimulation support of DDMS by its effective design. Future possibilities of enhancing this work have much direction. Our inspiration is to avoid the use of separate security protocols which are *attack specific*. In a practical world, the attackers tried in a single attack, and then he will not compromise on their host. Instead, they use a number of attacks of varying complexity will inevitably compromise the system. Instead, the two would be able to thwart the attack, DDMS embrace such a security protocol.

B. Future Enhancements

A future research should be to extend the proposed detection & mitigation of sinkhole attacks in wireless sensor network mechanism by incorporative data from several attack types and origin to further enhance to oppose old or new attacks. Also as a part of future research work on completing detection & mitigation of sinkhole attack is to be carried out.

References

[1] *Akyildiz Is W, Sankuru Subramanian Y, Cayirci E, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.*

[2] *Banerjee, Sudipto, Melanie M. Wall, and Bradley P. Carlin. "Frailty modeling for spatially correlated survival data, with application to infant mortality in Minnesota." Biostatistics 4, no. 1 (2003): 123-142..*

[3] *Choi, Byung Goo, Eung Jun Cho, Jin Ho Kim, Choong Seon Hong, and Jin Hyoung Kim. "A sinkhole attack detection mechanism for LQI based mesh routing in WSN." In Information Networking, 2009. ICOIN 2009. International Conference on, pp. 1-5. IEEE, 2009.*

[4] *Chan, Haowen, and Adrian Perrig. "Security and privacy in sensor networks."computer 36, no. 10 (2003): 103-105.*

[5] *Diggle, P. J., P. J. Ribeiro, and Model-based Geostatistics. Springer Series in Statistics. Springer, 2007.*

[6] *Heinemann W.B, Chandra kasha A.P, Balakrishnan H, et al., An application-specific protocol architecture for wireless micro sensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.*

[7] *Krontiris, Ioannis, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. "Intrusion detection*

of sinkhole attacks in wireless sensor networks." In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics, pp. 150-161. Springer Berlin Heidelberg, 2007..

[8] Krontiris, Ioannis, Thanassis Giannetsos, and Tassos Dimitriou. "Launching a sinkhole attack in wireless sensor networks; the intruder side." In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,, pp. 526-531. IEEE, 2008.

[9] Mhatre, Vivek P., Catherine Rosenberg, Daniel Kofman, Ravi Mazumdar, and Ness Shroff. "A minimum cost heterogeneous sensor network with a lifetime constraint." IEEE Transactions on Mobile Computing 4, no. 1 (2005): 4-15.

[10] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks."Computer Communications 30, no. 11 (2007): 2353-2364.

[11] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47, no. 6 (2004): 53-57.

[12] Roy, Suman Deb, Sneha Aman Singh, Subhrabrata Choudhury, and Narayan C. Debnath. "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management." In Computers and Communications, 2008. ISCC 2008. IEEE Symposium on, pp. 537-542. IEEE, 2008.

[13] Swami, Ananthram, Qing Zhao, Yao-Win Hong, and Lang Tong, eds.Wireless Sensor Networks: Signal Processing and Communications. John Wiley & Sons, 2007.

*[14] Bastian Bellman, "**Understanding network Hacks**", published by Springer PP15-24.*

*[15] Bijou Isaac and Neumann Iskar, "**Case Studies in Secure computing Achievements and Trends"** published by CRC Press PP10-20.*

*[16] Mohamed lbnkahla," **Wireless Sensor networks A cognitive perspective",** published by CRC Press PP 11-30.*

*[17] Dr.sudipmisra, "**Guide to Wireless Sensor Network**", published by Springer PP13-30.*

[18] Salam, Mohammad Abdus, and Alfred Sarkodee-Adoo. "Referencing Tool for Reputation and Trust in Wireless Sensor Networks." arXiv preprint arXiv:1508.01430 (2015).

[19] Panigrahi, Niranjan, and Pabitra Mohan Khilar. "An evolutionary based topological optimization strategy for consensus based clock synchronization protocols in wireless sensor network." Swarm and Evolutionary Computation22 (2015): 66-85..

*[20] Dr.Nabzanoon , Dr. Nash at Alb dour, Dr. Hated , Hematite S.A, and Rash amah's Al-Tara wanes, "**Security Challenges A s A factor Affecting The security of MANET: Attacks And Security solution"**, International Journal of Network Security & Its Application , Volume 7-Number 3,May 2015.*