International
Journal
Of Advanced Research in Engineering & Management (IJAREM)

BLACK HOLE Attack: A NEW Detection Technique

WAJAHAT GH MOHD[1], Meena Chaudhary[2], Musheer vaqur[3], Diwaker Mourya[4]

Abstract: Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. This paper proposes a technique to detect the black-hole attack using multiple base-stations and a check agent based technology. This technique is Energy efficient, Fast, Lightweight and Reduces message complexity. An effective solution is proposed that uses multiple base stations to improve the delivery of the packets from the sensor nodes reaching at least one base station in the network, thus ensuring high packet delivery success. The proposed technique is more efficient than the previous techniques and gives better results. Check agent is a software program which is self-controlling and it moves from node to node and checks the presence of black-hole nodes in the network. Routing through multiple base stations algorithm is only activated when there is a chance of black-hole attack on the network. This method prevents the black hole attack imposed by both single and multiple black hole nodes. The tool used to implement the proposed algorithm is NS2, which is an object oriented event drive software package. The result of the simulation study expected to get good network performance by minimizing the packet losses as well as effectively prevent the black hole attack against wireless sensor networks. A solution to avoid the blackhole attack has been proposed. The solution will be implemented in NS-2.

Keywords— WSN, Black-hole attacks, multiple base stations & Check agent..

I. INTRODUCTION

Wireless Sensor Network (WSN) provide a new model for sensing and dispersing information from various environments, aiming to serve numerous and different applications. Due to the continuous advancements, the wireless sensor networks have been recognized as the most fundamental advancement of the century. This is the outcome of the recent advances in electronic sensors, communication technologies and computation algorithms. Wireless sensor networks(WSNs) comprise of an extensive number of autonomous,sensing, computing, and communication elements that give a user or administrator the ability to instrument, observe, and react to react to events and phenomena in a specific environment. The wireless nodes envelop embedded electronic sensors along with battery and RF devices. The purpose of these sensors is to sense and recognize diverse biological parameters, for instance, temperature, pressure, air pollution etc, to communicate with the neighbouring nodes and compute the gathered data. Their application space is huge as they can be deployed in various fields like agriculture monitoring, smart homes , structures, target tracking, health care, military surveillance and earthquake observation and so on. In spite of the fact that WSNs are utilized with in numerous provisions, still they pose some limitations, which incorporate constrained energy supply, restricted computation and communication abilities. These limitations ought to be looked into while outlining protocols for WSNs. On account of these considerations particular to WSNs, numerous routing schemes using end-to-end devices and MANET are in appropriate for WSNs. A wireless sensor network (WSNs)is a network including hundreds or thousands of sensors nodes which are densely deployed in an unattented environment possessing the sensing capabilities, wireless communications and computations. Proper and careful planning is must to deploy the nodes in a wireless sensor network. Wireless communication and MEMS are the two advances which have brought an incredible revolution and have contributed highly in the development of wireless sensor networks. These systems contain sensor nodes that collect, process, store, and transfer information from one node to another. These nodes frame a network through which sensor readings can be propagated. Since the sensor nodes have some intelligence, data can be processed as it flows through the network. Wireless networks can be categorized into two types: infrastructure network and ad-hoc network. As

the name recommends, infrastructure geographically and perform communication simultaneously. When it goes out of range of one base station, it units with the new base station and starts communication through it. This whole phenomenon is termed as handoff. In contrast to this, mobile ad hoc network is a group of wireless mobile nodes in which nodes in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless communication. Ad hoc networks require no fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively setup as needed.

II. SECURITY IN WSN

There are numerous sensor system provisions like such ecological information accumulation, security observing, therapeutic science, military, tracking and so on when sensor systems are arbitrarily conveyed in a nature's domain, security gets to be amazingly imperative component. Since sensed information of sensor hubs is inclined to distinctive sorts of pernicious before arriving at base station.

Security mechanisms are required in correspondence a piece of the systems to give safe information.

Security in WSNs could be characterized as the technique for ensuring a prospective requisition against all known sorts of attacks. Attacks including Denial- of Service (DOS), traffic analysis, multiple identity/node replication, confidentiality and physical tampering are all ranges for concern inside WSN security structural planning outline.

The objective of confidentiality is required in sensors environment to protect information traveling among the sensor nodes of the network or between the sensors and the base station from disclosure.

Undoubtedly, WSNs are prone to different sorts of compromises that explore known and obscure vulnerabilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data that resides in these networked systems.

While the greater part of dangers could be managed through cryptographic materials provided by key administration conventions, some different dangers, such as node replication attacks, can in any case go imperceptible. Nodes replication attacks are one of the most redoubtable attacks, where an attacker compromising a node, uses its secret cryptographic key materials to successfully populate the network with clones of it.

III. SECURITY REQUIREMENTS

The crucial component to the success of mission- critical applications working in unattended WSN applications is Communication security. There are significant security prerequisites for WSNs to ensure that the network functions correctly and securely as purposed:

A. Authenticity

Authenticity empowers a sensor to guarantee the identities of its communicating entities with the goal that no enemy could disguise another entity, and perform forging. Here, the adversary can make receiving node accept that the information originates from an authentic source.

B. Confidentiality

Confidentiality ensures that the content of the message being exchanged is never unveiled to unauthorized entities. Network transmission of sensitive information requires confidentiality. On numerous applications, the nodes need to communicate exceptionally confidential data hence, it is very important to fabricate a secure communication channel in WSN.

C. Integrity

Integrity guarantees that a message being exchanged is never altered by an intruder without being distinguished. Data integrity serves to guarantee that the appropriated information have not been changed in transit.

D. Data Freshness
Data freshness recommends that the data is latest, and assures that no old message has been resent. This necessity is particularly imperative when imparted keys systems are continuously utilized. Typically, shared keys need to be renewed over time.

IV. ATTACKS IN WSN

In order to appreciate the challenge of securing a WSN against attack, it is important to think about the conceivable dangers to its security. There are a vast and expanding number of dangers and strike to which WSNs are susceptible. The various kinds of attacks are explained as:

A. Denial of Service
Denial of Service (DoS) is processed by the unintentional disappointment of nodes or malicious action. Here, the resources are exhausted by sending additional unnecessary packets and thus prevents legitimate users from gaining access to the services or resources. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

B. Black hole/Sinkhole Attack
In this attack, a pernicious node acts as a black- hole to lure all the traffic in the sensor network. Particularly in a flooding based convention, the assailant listens to demands for routes then answers to the target nodes that it holds the high caliber to the base station. Once the malicious device has capacity to embed itself between the communicating nodes, it is able to do anything with the packets passing between them. Indeed, this attack can influence even the nodes those are extensively a long way from the base stations.

C. Warm Hole Attack
In a warm-hole attack, the messages are taken from one part of the network to another through a low latency link via virtual tunnel made by an adversary. The easiest instance of this attack is when one node is found between two other nodes that are forwarding. However, wormhole attacks commonly involve two distant nodes that are conspired to underestimate the distance between them and forward packets through an outside correspondence channel that is only available to the adversary.

D. Node Replication Attack
In a node replication ambush, an assailant endeavors to add a node to a current WSN by replicating the node identifier of an officially existing node in the system. A node recreated and joined in the system in this way can conceivably cause extreme interruption in message correspondence in the WSN by defiling and sending the bundles in wrong courses. This may likewise prompt system partitioning, correspondence of false sensor readings. Likewise, if the attacker picks up physical access to the whole system, it is feasible for him to duplicate the cryptographic keys and utilize these keys for message correspondence from the recreated hub. The attacker can additionally put the repeated hub in strategic locations in the system with the goal that he could easily manipulate a a particular section of the system, perhaps bringing about a system partitioning.

Causes of node replication attack are as follows:
• It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member.
• It creates various attacks by extracting all the secret credentials of the captured node.
• It corrupts the monitoring operations by injecting false data.
• It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too.
• It is difficult to detect replicated node and hence authentication is difficult.

V. PROPOSED SCHEME

A. Objectives
The objective of confidentiality is required in WSN environment to avoid the disclosure of the data going around the sensor nodes of the system or between the sensors and the base station.

The objectives of the work are as:
The present work emphasizes on achieving the following objectives:
1. To detect and prevent black hole attack
2. To reduce the energy consumption in the network
3. To improve the lifetime of the network
4. To increase the throughput of the network

B. Proposed Method
The overall goal of the security solutions for WSN is to provide security services including authentication, confidentiality, integrity, anonymity, and availability to the mobile users. From the security design perspective, the WSNs have no clear line of defence. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well-defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols, such as AODV, DSR and wireless MAC protocols, such as 802.11, typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

The security problems are all related to malicious nodes that intentionally damage or compromise network functionality. However, selfish nodes, which use the network but do not cooperate to routing or packet forwarding for others in order not to spill battery life or network bandwidth, constitute an important problem as network functioning entirely relies on the cooperation between nodes and their contribution to basic network functions. To deal with these problems, the self-organising network concept must be based on an incentive for users to collaborate, thereby avoiding selfish behaviour.

C Methodology
step1. deployment of nodes
step 2. broadcast the route request messages to find the routes
step 3. destination replies via possible routes with route reply message
step 4. find the shortest path
step 5. give identity to the nodes in shortest path
step 6. if malicious node attacks, check its identity
step 7. if identity is different from the nodes which are in the shortest path then discard the packet
step 8. after packet discard, send route confirmation message
step 9. continue with regular data transmission from source to destination

VI. EXPERIMENTAL RESULTS

The proposed method has been implemented in NS 2 and the experimental results have been presented.

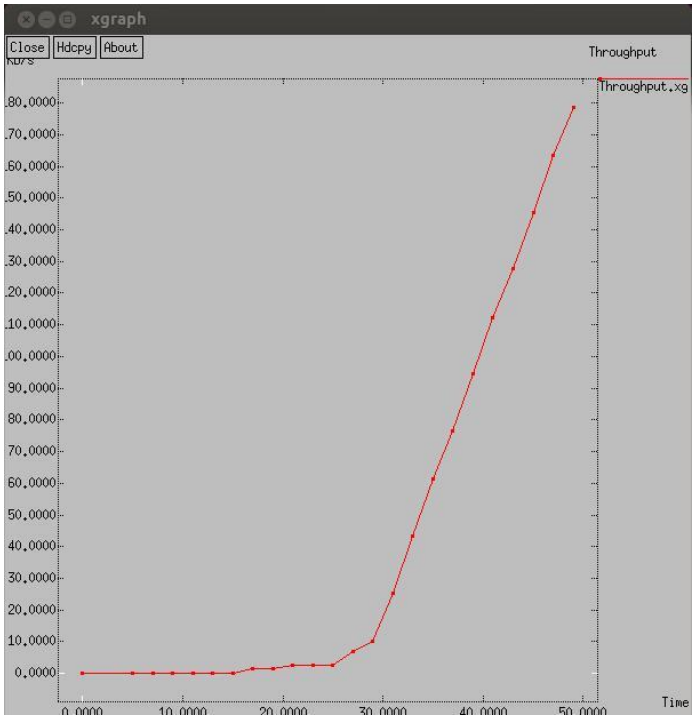

Fig. 1 Increase Throughput

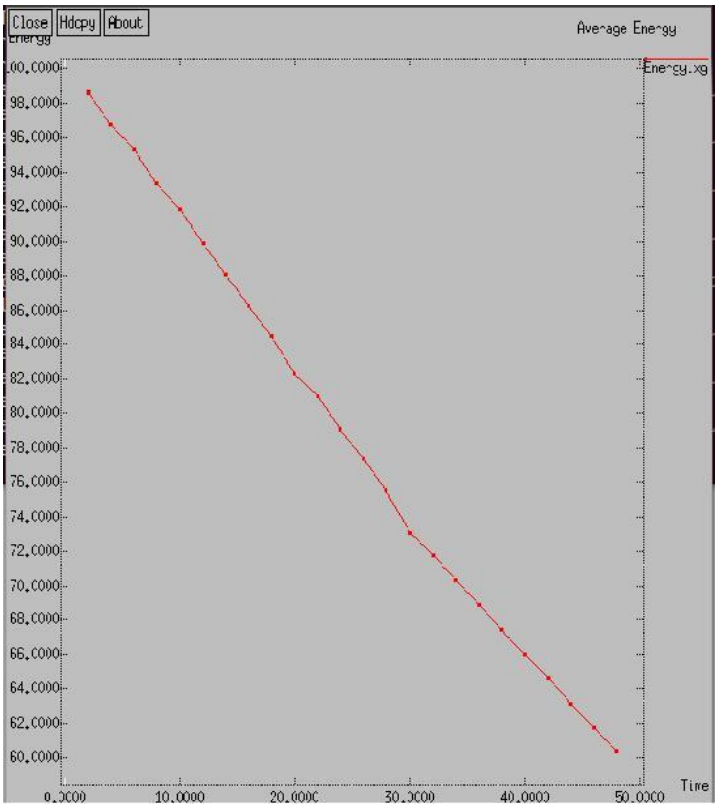

Fig. 2 Avarage Energy

Above graph shows the average energy consumed in the network. Initially 100 joules of energy was assigned to nodes deployed in the network. After running the simulation for 50 sec, energy remaining was found to be 60 joules. In the base paper, malicious node - ID broadcasting method is used. During broadcasting a lot of energy is consumed. In our study we used ID checking mechanism at the one path thick nodes so avoiding the broadcasting method saves energy. This eventually increases the network lifetime.

VII. CONCLUSION

The work presents the state that we studied the problem of sensor localization in the presence of malicious adversaries. We studied the problem of cooperative black hole attacks in WSN routing. The MN-ID broadcasting method provides improved performance of throughput packet delivery ratio and reduced packet loss. Therefore MN-ID broadcasting methods provide improved network performance and minimum packet loss in the packet transmission. For each category, an analysis has been carried out for each scheme highlighting their advantages and drawbacks. Finally, some important future research opportunities are pointed out for the future research.

ACKNOWLEDGMENT

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1]. H.Weerasinge and H.Fu ―Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implimentation and evaluation‖international journal of software engg. and its applications,vol2,no3 in MANET‖, Journal Of Networks, Vol. 3, NO. 5,

[2]. Jian Yin, Sanjay Madria, ―A Hierarchical Secure Routing Protocol against Black Hole‖, IEEE SUTC 2012 Taiwan, 5-7 June 2012

[3]. Dokurer, S.; Ert, Y.M.; and Acar, C.E. (2011). Performance analysis of ad hoc networks under black hole attacks. SoutheastCon, 2011, Proceedings IEEE, 148 – 153.

[4]. Dr. Karim Konate and Abdourahime Gaye(2011),„a proposal mechanism against the attacks: cooperative black hole, blackmail, overflow and selfish in routing protocol of mobile ad hoc network‟, international journal of future generation communication and networking Vol. 4, No. 2

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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

[9]. 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.

[10]. 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

[11]. 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;

[12]. S. Sharma and R. Gupta, (2012) ―Simulation study of black hole attack in the mobile ad-hoc networks,‖ journal of engineering science and technology, vol. 4, no. 2 pp. 243-250.