Efficient Intrusion Detection in Wireless Sensor Networks using Peer Interaction Assessment Algorithm

G. Pradeep Kumar, Ashif Ismail Sheriff K, M. Keerthinath, M. Kundru Malai Rajan

***Abstract*— Wireless sensor networks are typically used out in an open, uncontrolled environment, often in hostile territories. In particular, several important applications for such networks come from military and defense arenas. Use of wireless medium and inherent collaborative nature of the network protocols make such network vulnerable to various forms of attacks wherein malicious nodes are deployed into the network and launch various attacks. These nodes are collectively called compromised nodes. In this paper, we first analyse the unique features of wireless sensor networks and discuss the challenges for compromised nodes detection. Then we propose a hybrid algorithm for detecting sinkhole attacks and wormhole attacks for wireless sensor networks. Security in Wireless Sensor Networks (WSNs) is especially challenging and quite different from traditional network security mechanisms. Existing algorithms use a mapping process in order to create a fixed route for data travel, and looks for forbidden structures in the connectivity graph. Here we provide an intrusion detection system based on study of the transmission and reception densities of the nodes. This system works based on the study of the density of packet transmissions and packet receptions for forming a suspicious set, consisting of all the nodes with mistrustful conduct. This narrowed-down list is further verified by studying the characteristics of the one to one interaction of the suspicious nodes with their neighbours and the unidirectional communication exhibited by the malicious nodes acts as the diagnosis point of this process.**

***Index Terms*— Intrusion detection, sinkhole attack, sensor network, wireless network.**

I. INTRODUCTION

A wireless sensor node, also called mote, is a computational device that has sensing device, processor, transceiver, memory, and power supply. The sensing devices sense the environment and gather the data that represent the physical conditions being monitored. The sensor readings are sent to the local processor for preliminary processing and then sent to the base station in a multi-hop wireless communication manner for further processing. Motes are programmed with the appropriate operating parameters and security credentials before deployed. In order to obtain detailed and integrated data, a large number of sensor nodes are generally distributed over the area interested and form a wireless sensor network. Wireless sensors have a variety of applications, including battlefield surveillance, environmental monitoring, medical applications, and space applications.

G. Pradeep Kumar is working as , [1]Assistant Professor, Velammal College of Engineering and Technology, Madurai, India, **Ashif Ismail Sheriff K, M. Keerthinath and M. Kundru Malai Rajan are** UG students, Velammal College of Engineering and Technology, Madurai, India, Emails: prad.mypassion@gmail.com , ashif.sheriff@gmail.com , ptm.keerthinth@gmail.com , rmkrajan@gmail.com .

Security is critical for many of these applications. Moreover, many wireless sensor networks are deployed in an unattended and hostile environment. Therefore, wireless sensor networks are subjected to various kinds of attacks.

Most of the applications in wireless sensor networks (WSN) require the unattended operation of a large number of sensors. This fact along with the limited computational and communication resources of their nodes make them susceptible to attacks. Sensor networks cannot rely on human intervention to face an adversary's attempt to compromise the network or hinder its proper operation. Instead, an autonomic response of the network that relies on the embedded pre-programmed policies and a coordinated, cooperative behavior is the most effective way to gain maximum advantage against adversaries.

There are two major types of attacks that are possible and are taken into consideration in our algorithm. They are sinkhole attacks and wormhole attacks.

In a Sinkhole attack a compromised node tries to draw all or as much as possible traffic from a particular area, by making itself look attractive to the Intrusion Detection of Sinkhole Attacks in WSN surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station. By taking part in the routing process, she can then launch more severe attacks, like selectively forwarding, modifying or even dropping the packets coming through. A compromised node does not necessarily have to target other nodes from areas outside its neighborhood in order to control traffic. The adversary needs only to launch the sinkhole attack from a node as close as possible to the base station. In this case, by having the neighboring nodes choose the intruder as their parent, all the traffic coming from their descendants will also end up in the sinkhole. So the attack can be very effective even if it is launched locally, with small effort from the side of the attacker.

The wormhole attack goes by a similar process for advertising its location but the difference here is that instead of dropping the packets, it selectively retransmits them to the other end of the wormhole that can efficiently lie anywhere in or outside the network. After the attacker attracts a lot of data traffic through the wormhole, it can disrupt the data flow by selectively modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically, etc. The attacker can also simply record the traffic for later analysis. Thus losing essential or sensitive data to an external intruder.

Hence a single malicious node could be very damaging, since its effects are not localized, rather affects the performance of the entire system as such. Hence detection of malicious nodes is of utmost importance. This system takes an amalgamated approach in dealing with malicious node. That is, it provides a hybrid algorithm which can deal with both sinkhole and wormhole nodes. It is a two-step process which proceeds by first forming a suspicious set based on traffic audit and then determining the malicious nodes based on one on one interaction with their neighbors by response checking.

II. RESEARCH ISSUES

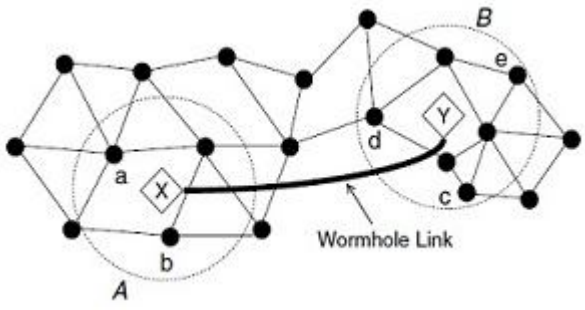
Wormholes are particularly hard to detect as they blend in with the system. The same becomes even more complex when it comes to sinkholes, because normal nodes existing in the system can be made corrupt by reprogramming them into sinkhole nodes. Since these corrupt nodes can overcome any type of routing protocol to advertise their node, it will not help to recreate the routing protocol. One of the existing methods uses a connectivity graph to ascertain the ideal data flow in tha network. Detection of wormholes I done by looking for illegal structures in the connectivity graph. Systems like these are possible only for small scale systems, and do not take into account nodes with longer ranges and selective retransmission across two networks.

Other methods include the use of mobile agents for monitoring, which are high on energy consumption and are prone to false alarms. Sinkhole detection algorithms like overhead traffic audit and packet analysis are very tedious and time consuming.

III. EXISTING METHODS

A. Unit Disk Graph Model

In unit disk graphs (UDG) each node is modeled as a disk of unit radius in the plane, modeling the communication range of the node with Omni-directional antenna. Each node is a neighbor of all nodes located within its disk. Hence a link structure is formed linking all the nearby nodes that lie within the circle. Any data packet is assumed to travel only through the links found in the connectivity graph. This method is specifically adopted for the detection of wormholes, and this is done by looking for forbidden substructures in the connectivity graph that should not be present in a legal connectivity graph. This method is restricted for small area



networks and does not take into consideration heterogeneous nodes.

B. Network Monitoring

Network monitoring is one of the most commonly used methods for detecting sinkhole attacks in WSN. Each Intrusion Detection System client listens on the network and captures and examines individual packets passing from its immediate neighborhood in real time. Since all communication in a WSN is conducted over the air, and each node can overhear the traffic in its neighborhood, this is a natural audit source for the IDS client. But the process of packet analysis is very tedious and energy consuming. Also it requires the nodes to be active all the time which further drains their batteries.

C. Mobile Agent

In conventional detection systems use of an external monitoring agent called as a mobile agent is employed in order to detect the presence of malicious nodes in the existing network. This mobile agent is like a flood packet and it is passed on from one node to another until it reaches the destination. The alterations done to the packet is used to deduce the location of the malicious node. The main drawback here is high power consumption and really high false alarms.

IV. PROPOSED METHOD

The placement of wormhole influences the network connectivity by creating long links between two sets of nodes located potentially far away. The resulting connectivity graph thus deviates from the true connectivity graph. Our detection algorithm essentially looks for forbidden substructures in the network. Since the algorithm is designed for sinkhole attacks also, the algorithm should be made to focus on packet dropping. But concentrating on the packet traits of all the nodes and classifying it is a tedious and time consuming process. Moreover it would be enough and sufficient to detect a node as malicious, since any type of malicious node is to be eliminated. For this purpose we follow a two-step process. The strategy adopted here is to study the incoming packet traffic for all the nodes rather than studying the outgoing packet traffic. Hence in our algorithm, the first step is to form a suspicion set, which comprises of all the nodes deemed suspicious. The second step involves proper detection of the malicious node by interaction with the node.

A. Neighbour detection

The first step in intrusion detection is to have a first-hand information on the valid neighbours of every node. It is known that the transmission range of a wireless sensor node is limited. Hence accessing all the nodes from a localized node point is not practically implementable. Hence any information regarding intrusion can be validated only through its neighbours. The process of neighbour detection has the following steps

- For every node in the network, calculate its distance from all other nodes.
- Arrange the distances in ascending order
- Find the median by choosing the center value of the list
- Choose all the nodes with distances less than the median distance as valid neighbors.

- Repeat this for all the nodes in the network.

ALGORITHM 1: Inter Node Distance Calculation

1: **if** *Distance of node n_i from node n_i* **then**

2: *Distance* ⟵ *0*

3: **else** *Distance of node n_i from node n_j*

4: *calculate the distance using the formula* $Distance=\sqrt{[(x_j-x_i)^2+(y_j-y_i)^2]}$

5**: end if**

6: **if** *two nodes taken are not the same*

7: **if** *Distance of node i from node j is less than median distance*

8: *Node j is a neighbour of Node i*

9: **end if**

10: **end if**

B. Suspicion set Formation using tabling algorithm

The formation of the suspicion set is done after the complete analysis of all the nodes by studying the incoming packet densities for each of the nodes. The traffic audit is carried out individually for the incoming and outgoing packets for each of the nodes by themselves and this is overlooked by the cluster head node. Hence the need for any mobile agent or other external means has been effectively eliminated for the suspicion set formation.

- Create an independent routine for packet monitoring in each node.
- This routine is run every time transmission or reception takes place.
- A trigger point is set with respect to a specific ratio reached between the thresholds of the transmission and reception levels.
- Once it is triggered, add to suspicion set.

ALGORITHM 2: Tabling Algorithm

1: **if** *node is active*

2: **if** *Trigger point for number of receptions over the number of transmissions is reached*

3: *Node is added to the suspicious set*

4: **end if**

5: **end if**

C. Detection of Unauthorised cluster heads

Most of the reporting is done to the cluster head. Hence a high amount of possibility lies in a malicious node trying to impersonate a cluster head. This would facilitate the intruder to gain access of all the nodes inside the range. Also, any intrusion detection routine is triggered only by the cluster head, which can be essentially stopped by the malicious node. Hence, this act should be prevented, and more importantly, this gesture can be used as a means to detect a malicious node.

ALGORITHM 3: Detection of Unauthorised cluster heads

1: **while** *connecting with cluster head*

2: **if** *coordinate of the cluster head node is not the same as the stored value*

3: *report to previous cluster head*

4: *add to suspicious set*

5: **end if**

D. Malicious node Detection by peer interaction assessment

In a network with a large number of nodes, we are left with a few nodes in the suspicion set. Hence the job of intrusion detection becomes much easier. The next step is the confirmation phase. This step is brought about by one to one interaction with the node under suspicion. In the beginning, the cluster head identifies the node belonging to its cluster that has been listed under the suspicious set. Next the cluster head commands all the nodes in that cluster to send a packet to the suspicious nodes. This packet is a special high priority packet which demands immediate reply to the sending node. But a malicious node like a sinkhole or wormhole node can only receive but not transmit. Hence those nodes will not be able to reply to the packet request. This is checked by the valid neighbors of the suspicious node and duly reported to the cluster head. If a proper reply is obtained, it is discarded. Else, preventive measures are taken.

ALGORITHM 3: Peer Response Analysis

1: **for** *all nodes in suspicion set*

2: *Send packet p1 and request immediate reply*

3: **if** *reply is obtained*

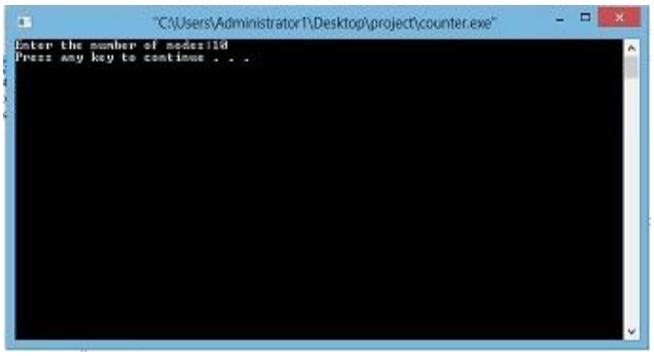
4: *Remove from suspicious set*

5: **End if**

6: **Else** *the node n_i is a malicious node*

V. RESULTS

Node creation:



Coordinates of nodes in the network:

```
The coordinates of node 1 :     41      5
The coordinates of node 2 :     67      45
The coordinates of node 3 :     34      81
The coordinates of node 4 :     0       27
The coordinates of node 5 :     69      61
The coordinates of node 6 :     24      91
The coordinates of node 7 :     78      95
The coordinates of node 8 :     58      42
The coordinates of node 9 :     62      27
The coordinates of node 10 :    64      36
```

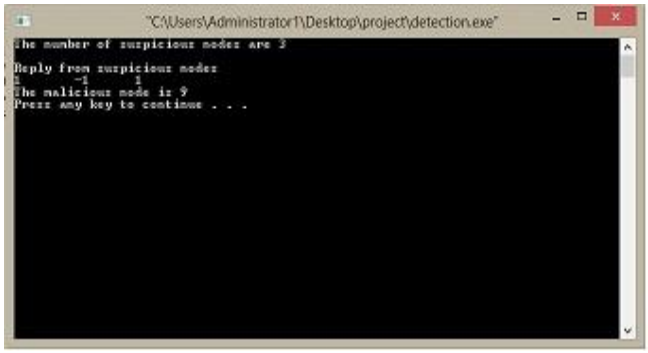
```
Distance of node 1 from other nodes...
0
47.7074
76.3217
46.5296
62.6099
87.6641
97.3088
40.7185
30.4138
38.6005
```

Neighbour detection:

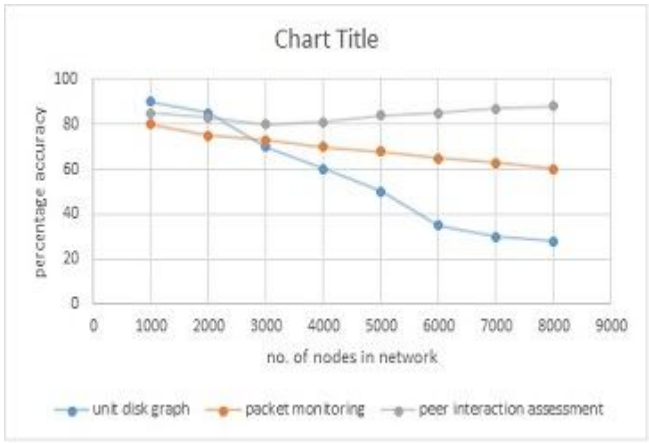
```
Neighbour nodes of Node 1 are... 2      4       8       9       10
Neighbour nodes of Node 2 are... 1      3       5       8       9       10
Neighbour nodes of Node 3 are... 2      5       6       7       8
Neighbour nodes of Node 4 are... 1
Neighbour nodes of Node 5 are... 2      3       7       8       9       10
Neighbour nodes of Node 6 are... 3
Neighbour nodes of Node 7 are... 3      5
Neighbour nodes of Node 8 are... 1      2       3       5       9       10
Neighbour nodes of Node 9 are... 1      2       5       8       10
Neighbour nodes of Node 10 are... 1     2       5       8       9


The Suspicious nodes are        8       9       10
```

Malicious node detection by peer interaction assessment:



Comparison with existing methods:



VI. CONCLUSION

An ideal algorithm for cumulative detection of wormholes and sinkholes has been explained using a peer interaction assessment algorithm. A two-step process involving formation of suspicion set based on audit of the transmission and reception traffic of all the nodes that is overlooked by the cluster head followed by a peer interaction assessment of each suspicious node by its cluster head wherein the response of the suspicious node with its neighbours is used to efficiently detect the malicious nodes. This method is much more accurate and energy efficient when compared with the existing methods.

REFERENCES

[1] Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", pp. 271–278, August 1999.

[2] I. F. Akyildiz, S. Weilian, Y. Sankarasubramania and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8,pp. 102–114, August 2002.

[3] Z. Q. C. Yunxia, "On the lifetime of wireless sensor networks," Vol. 9, pp. 976–978, 2005.

[4] A.D. Wood, J.A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press,2004.

[5] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[6] Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[7] S.V.Manisekaran, R.Venkatesan, G.Deivanai "Mobile Adaptive Distributed Clustering Algorithm for Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887),Volume 20– No.7, April 2011.

[8] Shilpa Mahajan1, Jyoteesh Malhotra2 "Energy Efficient Path Determination in Wireless Sensor Network Using BFS Approach " Received September 9, 2011; revised October 10, 2011; accepted October 20, 2011

[9] Li-Liann Lu, Jean-Lien C. Wu, San-Hao Chen, "A Cluster-Based Algorithm for Redundant Nodes Discovery in Dense Sensor Networks", International Journal of Sensor Networks, 2011 Vol.10, No.1/2, pp.59 - 72

[10] H. Chan, A. Perrig, An emergent algorithm for highly uniform cluster formation, in: Proceedings of the 1st European Workshop on Sensor Networks (EWSN), Berlin, Germany, January 2004.

[11] O.Younis, S.Fahmy, A hybrid energy-efficient distributed clustering approach for Ad Hoc sensor networks, IEEE Transactions on mobile computing 3(4) (2004) 366-379.

[12] S.Bandyopadhyay, E.Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, April 2003.

[13] Y. Liu, Z. Lo, K. Xu and L. Chen; "A reliable clustering algorithm base on LEACH protocol in wireless mobile sensor networks" 2nd International Conference on Mechanical and Electrical Technology (ICMET), 2010, pp 692 – 696.

[14] X. Co, H. Zhang, J. Shi, and G.Cui "Cluster heads election analysis for multi-hop wireless sensor networks based on weighted graph and particle swarm optimization", in IEEE fourth International Conference on computing, 7, 599–603.

[15] R. Wang, L. Guozhi, and C. Zheng " A clustering algorithm based on virtual area partition for heterogeneous wireless sensor networks", in International Conference on Mechatronics and Automation, 372–376.

[16] Mehdi Saeidmanesh, Mojtaba Hajimohammadi, and AliMovaghar, "Energy and Distance Based Clustering: An Energy Efficient Clustering Method for Wireless Sensor Networks", World Academy of Science, Engineering and Technology, vol. 55, p.p 555-559, 2009.

[17] Stanislava, S. and Wendi, B. H. 2005. Prolonging the Lifetime of Wireless Sensor Networks via Unequal Clustering. In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, p.p 8-16.

[18] H.Chan, M.Luk, A.Perrig, Using clustering information for sensor network localization, in: Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS'05), Marina Del Rey, CA, USA, June 2005.