Event Identification for Wireless Sensor Network

Shimi K S
Department Of Computer Science Of Engineering
Sreenarayana Gurukulam College Of Enginnering
Ernakulam, India

Abstract- Wireless sensor networks consist of sensor nodes with radio, processor, memory, battery and sensor hardware. With widespread deployment of these devices one can precisely monitor the environment. Sensor nodes are resource constrained in terms of radio range, processor speed, memory and power. WSNs are mostly unguarded and the wireless medium is broadcast. This makes them more vulnerable to attacks. Without proper security measures, an enemy can launch various kinds of attacks in hostile environments. These attacks can disrupt the normal working of WSNs and can defeat the purpose of their deployment. Therefore security is an important aspect of these networks. WSNs are often deployed to monitor important emergency events, such as forest fire and battlefield monitoring. System Monitoring Modules (SMM) should be integrated with Intrusion Detection Modules (IDM). This integration can facilitate classification between malicious events and important emergency events. Unlike existing techniques, proposed system aims at addressing secure in-network aggregation problems from an intrusion detection perspective. Existing systems uses clustering, authentication mechanisms and cryptographic techniques for data aggregation in WSNs. These systems gives more priority to secure data aggregation than anomaly detection. Most of these systems assume that not more than one compromised nodes in the network. In the proposed system, if more than one malicious node is present, then also the false event is identified.

Index Terms- *intrusion detection system, Wireless sensor networks, IDM-SMM*

I. INTRODUCTION

Wireless sensor networks comprise a large number of tiny sensor nodes that have limited power, bandwidth, memory and computational capabilities. These inherent limitations of sensor nodes can make the network more vulnerable to faults and malicious attacks. A key challenge in identifying misbehaviors in wireless sensor networks is to develop algorithms for detecting anomalies in the network, such that these algorithms minimise their communication overhead and energy consumption in the network. Misbehaviors in the network can be identified by analysing the data from the sensor nodes. A node may show misbehaviours whenever a fault occurs or due to malicious activity by compromised sensors. In both cases, misbehaviors can be identified by analysing sensor or traffic measurements to discriminate normal behavior from anomalous behavior. Note that the underlying distribution of these measurements may not be known a priori. Therefore, anomaly detection in data with an unknown distribution is an important problem to be addressed in wireless sensor networks.

WSNs are often deployed to monitor important emergency events, such as forest fire and battlefield monitoring. To enhance WSN security, System Monitoring Modules (SMM) should be integrated with Intrusion Detection Modules (IDM). This integration can facilitate classification between malicious events and important emergency events. When node A raisesan alert on node B because of an event E, node A can further initiate investigation on event E. node A can wake up relevant sensor nodes around node B and request their opinions about event E. If the majority of sensor nodes think that event E could happen, node A can make a decision that event E is triggered by some emergency event. Otherwise, node A can suspect that event E is malicious.

II. RELATED WORK

Peng [1] present an interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised.

In a cluster-based technique [2] is used to detect routing attacks in sensor networks. In this approach each sensor node monitors the routing messages it receives. At regular intervals, each sensor node characterizes the set of routing records it has seen in terms of a vector of features. Fixed width clustering algorithm creates spherical clusters of fixed radius for a data set. Then the clusters are labelled normal if they contain more than a given fraction of the total data points; otherwise, they are labelled anomalous.

Wu *et al.* [3] propose a Secure Aggregation Tree (SAT) to detect and prevent cheating in WSNs, in which the detection of cheating is based on topological constraints in a constructed aggregation tree.

Chan *et al.* [4] present a secure aggregation scheme for arbitrary aggregator topologies and multiple malicious nodes. Yang *et al.* [5] propose a Secure Hop-by-hop Data Aggregation Protocol (SDAP) based on principles of divide-and-conquer and commit-and-attest.

III. PROPOSED METHODOLOGY

Proposed protocol is equipped with two modules: Intrusion Detection Module (IDM) and System Monitoring Module (SMM). The functionality of the IDM is to detect whether monitored nodes are malicious nodes, while the functionality of the SMM is to monitor important emergency events. SMM is a necessary component for most of WSN applications. Since WSNs are usually densely deployed, nodes close to each other can have spatially correlated observations, which can facilitate the collaboration of sensor nodes in proximity to differentiate

between malicious events and important emergency events. IDM and SMM need to be integrated with each other to work effectively. Relying on local detection alone is not desirable because each node has only very limited information available. Furthermore, since sensor nodes are prone to failure, it is very difficult to differentiate between emergency events sent by good nodes and malicious events.

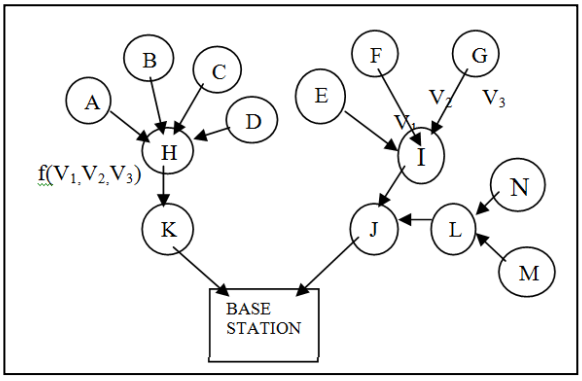

Figure 1 An Example Of Aggregation Tree

In this scheme, whenever IDM and SMM detect some abnormal events, they need to request the collaboration of more sensor nodes around the events in order to make a final decision. Node A promiscuously overhears its neighbor's transmitted aggregate value and compares it with the predicted normal range. If the overheard value lies outside the normal range, either an event E happens or the neighbor N then becomes a suspect. To tell whether node N is a malicious node or event E is an important emergency event like the outbreak of a forest fire, node A initiates the collaboration between IDM and SMM by waking up relevant sensor nodes around node N and requesting their opinions about event E.

IV. IMPLEMENTATION

Consecutive observations of sensor nodes are usually highly correlated in the time domain. This correlation, along with the collaborative nature of WSNs, makes it possible to predict future observed values based on previous values. This motivates our proposed local detection algorithms. Furthermore, since WSNs are usually densely deployed, nodes close to each other can have spatially correlated observations, which can facilitate the collaboration of sensor nodes in proximity to differentiate between malicious events and important emergency events. This motivates us to integrate SMM and IDM in order to achieve accurate detection results.

To utilize data aggregation, an aggregation tree is often built first. Figure 1is one example of such an aggregation tree. In Figure 1, nodes A, B, C, and D perform sensing tasks, obtain values and transmit them to their parent node H. Node H aggregates (min, max, sum, average, etc.) the received values from nodes A,B,C, and D, and transmits the aggregated value further up to node K. The same is true for operation (E, F,G) -> I -> J and operation (M,N) -> L ->J. These aggregation operations are performed based on the established parent-child relationship, which can be modelled using Figure 1. In Figure 1, the base station collects all these data and, if necessary, can transmit them across the Internet.

WSNs are often deployed to monitor emergency events like forest fire. Assume that the majority of nodes around some unusual events are not compromised. In anomaly based detection, the normal system behavior is defined as the behavior of the majority of nodes (or similarly, the behavior of the system in the majority of its operational time). By majority, it means that the number of these nodes is much larger than other (potentially compromised) nodes. This assumption is necessary to make any forward progress.

When node A raises an alert on node B because of some event E, to decide whether E is malicious or emergent, A may initiate a further investigation on E by collaborating with existing SMMs. To save energy, some sensor nodes are periodically scheduled to sleep. Based on this, node A can wake up those sensor nodes around B and request from these nodes their opinions on E. Whenever the opinion from the neighboring nodes are available, data aggregation operation is performed. That is, the values obtained by the neighboring nodes are undergoing the aggregation operation (min, max, average, etc). The aggregated value is compared with the value received earlier. If the difference is close to the threshold (threshold value is fixed manually) then the event is identified as emergency event.

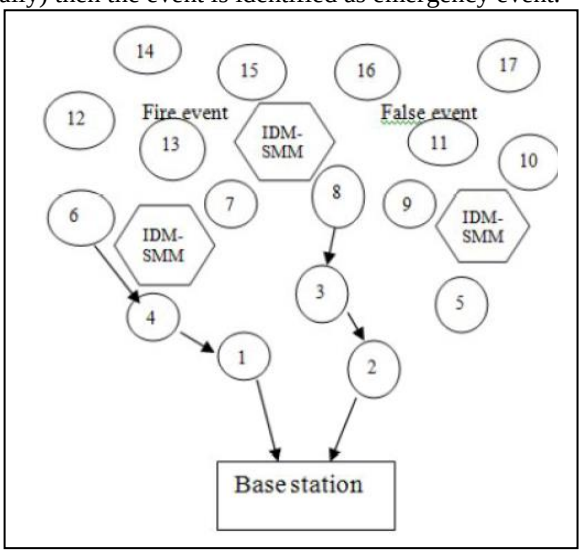

Figure 2 Collaboration between IDM and SMM

On the other hand, if A finds that the majority of sensor nodes think that event E should not happen, A then thinks that E is triggered by either a malicious node or a faulty yet good node. In this way, A can continue to wake up those nodes around event E and ask their opinions about E. the values obtained by the neighboring nodes are undergoing the aggregation operation (min, max, average, etc). The aggregated value is compared with the value received earlier. If the difference is lying outside the threshold (threshold value is fixed manually) then the event is identified as malicious event. After A makes a final decision, A can report this event to base stations.

The above mentioned method is feasible when only one malicious node is present in the network. When there is more

than one compromised nodes in the network, the opinion may contain more than one false opinion about an event. In this case, the decision can't be taken from the opinion by neighbors. Then IDM-SMM module comes in to action. IDM-SMM module is continuously monitoring the network. The compromised nodes will be acting abnormal to the messages sent by IDM-SMM module. Reply messages are not sent by the compromised nodes. These nodes are identified by the IDM-SMM module. When there is an event happens, IDM-SMM module verifies the opinions sent by the neighbour nodes and also identifies the misbehaving nodes in the network. This information is taken in to account for taking a decision about that event.

The IDM-SMM module will be monitoring the nodes coming under its range. This monitoring will be helpful to identify the misbehaving nodes in the network. Whenever an event happens, IDM-SMM module and the aggregation operation at the parent node will be work together to identify the event. Whether it's an emergency event or malicious event, it will be send to base station.

Set node three nodes as compromised nodes. That is, these nodes can inject falsified a data into a network. Intuitively, it is easier to detect attackers that have larger variations from normal nodes. These three nodes are identified and their activity of false event alerting is identified. Packet delivery ratio and throughput of the system will be low in the case of multiple compromised nodes. These are tested under NS2 background.

V. CONCLUSION AND FUTURE WORK

Security in wireless sensor networks is an important problem. To enhance WSN security in this system, first proposed that the integration or broadcasting of IDM and SMM to provide intrusion detection capabilities for WSNs. Then introduce local detection mechanism (data aggregation operation on values from neighboring nodes) to detect false injected data. Further demonstrated how the proposed IDM can work together with SMM to differentiate between malicious events and emergency events when multiple neighbouring nodes become malicious.

The method is suitable for lesser number of malicious nodes when compared to the normal nodes. Method should be enhanced to work properly if the number of compromised nodes increases.

REFERENCES

[1] Sencun Zhu, Sanjeev Setia, Sushil Jajodia and Peng Ning "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks" IEEE Symposium on Security and Privacy proceedings 2004.

[2] C. Loo et al., "Intrusion Detection for Routing Attacks in Sensor Networks," Int'l. J. Distrib. Sensor Networks, vol. 2, no. 4, 2006, pp. 313–32.H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[3] K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", *Elsevier AD HOC Networks Journal, Special Issue on Security Issues in Sensor and AD HOC Networks*, Vol. 15, No. 1, 2007, pp. 100-111

[4] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical InNetwork Aggregation in Sensor Networks," *ACM CCS'06*, Alexandria, VA, 2006, pp. 278-287

[5] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," *ACM MOBIHOC'06*, Florence, Italy, May 2006, pp. 356-367.

AUTHORS

First Author – Shimi K S, MTech, Sree Narayana Gurukulam College of Engineering, shimi.sivadas@gmail.com