International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 11, November 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

ANALYSIS OF DATA SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS USING NETWORK SIMULATOR

A. Senthil Kumar[1], Dr. E. Logashanmugam[2]

[1]*Research Scholar, St. Peter's University, Avadi – Chennai (India)*

[2]*Professor & Head of ECE , Sathyabama University, Chennai (India)*

ABSTRACT

The resource-constrained sensors in mission-critical applications are subject to both random failures and intentional compromise by the adversary, which poses severe security threats in wireless sensor networks (WSNs). The different types of security threats have been identified and addressed in an individual manner in the past. And most solutions are cryptography based. In this paper, we argue that cryptography alone is insufficient to fully address the insider attacks in the existence of both the compromised and faulty sensor nodes. We further propose a proactive data security framework (PDSF) to identify compromised and faulty nodes proactively and prohibit them from participating network activities in a dynamic manner. PDSF is aimed to serve as the front line in defending against all different types of security threats. The rationale behind our approach is that a sensor's future behavior can be predicted (at least) probabilistically by its past behavior. PDSF is divided into two key modules, that is, misbehavior characterization & monitoring, and trust management. PDSF characterizes different types of misbehavior in WSNs and defines a set of monitoring criteria. PDSF further develops a trust management model, which adapts to the resource constrained nature of the WSNs.

I. INTRODUCTION

We propose a hierarchical trust management protocol leveraging clustering to cope with a large number of heterogeneous SNs for scalability and reconfigurability, as well as to cope with selfish or malicious SNs for survivability and intrusion tolerance and also the node categorization algorithm to catch the packet droppers and modifiers present in the network. To deal with packet droppers, a widely adopted countermeasure is multipath forwarding, in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. To locate and identify packet droppers and modifiers, it has been proposed that nodes continuously monitor the forwarding behaviors of their neighbors to determine if their neighbors are misbehaving, and the approach can be extended by using the reputation based mechanisms to allow nodes to infer whether a non neighbor node is trustable.

This methodology may be subject to high-energy cost incurred by the promiscuous operating mode of wireless interface; moreover, the reputation mechanisms have to be exercised with cautions to avoid or mitigate bad mouth attacks and others. Recently all proposed a probabilistic nested marking (PNM) scheme. But with the PNM scheme, modified packets should not be filtered out en route because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes.

In this paper, we propose a simple yet effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs our proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

1.1 Existing System

Some recent works have paid attention to the presence of compromised and faulty sensors. These works focus on increasing security resilience, and use the scale and redundancy in the WSN to their advantage. These works usually introduce a threshold property to their designs to gain the resilience against up to a certain number of compromised and faulty nodes. However, the effectiveness of these passive approaches is suspicious in practice, where the predefined threshold parameter may deviate significantly from the practical situation. Furthermore, these works are limited in scope. They usually each deal with one individual type of insider attacks, and the corresponding solutions are highly specific and not applicable to other attacks. A number of different solutions are thus demanded to address different types of insider attacks and node random failures. This is extremely inefficient if not impossible in WSNs due to lack of resources, not to mention the compatibility issue and repetitive designs.

1.2 Drawbacks of Existing System

The existing cryptography technique does not have solutions for following solutions

- Message delay attack
- Message collision attack
- Bogus data attack
- Selective forwarding attack

1.3 Proposed System

1.3.1 Misbehavior Characterization and Monitoring

The misbehavior of the node is characterized by using the node categorization algorithm. In our project we are considering the packet droppers and packet modifier attack.

1.3.2 Node Categorization Algorithm

The node categorization algorithm categorizes the wireless nodes. It depends on the behavior of those nodes whether it is giving the good throughput or average. It helps to know about the sensor nodes.

1.3.3 Trust Management Model

We apply hierarchical trust management to trust-based intrusion detection as another application. We first describe the algorithm that can be used by a high-level node such as a CH (or a base station) to perform trust-based intrusion detection of the SNs (or CHs respectively) under its control. Then we develop a statistical method to assess trust based IDS false positive and false negative probabilities. Without loss of generality, in this section we illustrate how a CH performs **trust-based intrusion detection** on SNs in its cluster. A similar treatment applies to a base station performing trust-based intrusion detection on CHs in a WSN.

II. WIRELESS SENSOR NETWORK

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

III. NETWORK SIMULATOR

Network Simulator (NS) is a simulation tool targeted at both wired and wireless (local and satellite) networking research. NS is a very promising tool and is being used by universities and researchers. In this report we provided information how to install NS2 on UNIX and Windows. Then we discussed how to use NS2 to simulate wired and wireless networks. A simple but limited method is to combine the existing components with OTcl scripts; a complex but powerful method is to implement new components into NS2 using C++. We discussed both of the two methods. Finally, the methods to animate (using NAM) and to analyze (using Xgraph/Gnuplot) the simulation results are presented.

IV. A PROACTIVE DATA SECURITY FRAMEWORK (PDSF)

This project is divided into two major modules as given below

Module 1- Misbehavior characterization and monitoring

Module 2 - Trust management.

4.1 Module - 1 Misbehavior Characterization and Monitoring

The misbehavior of the node is characterized by using the node categorization algorithm. In our project we are considering only the packet droppers and packet modifier attack. The al ed below.

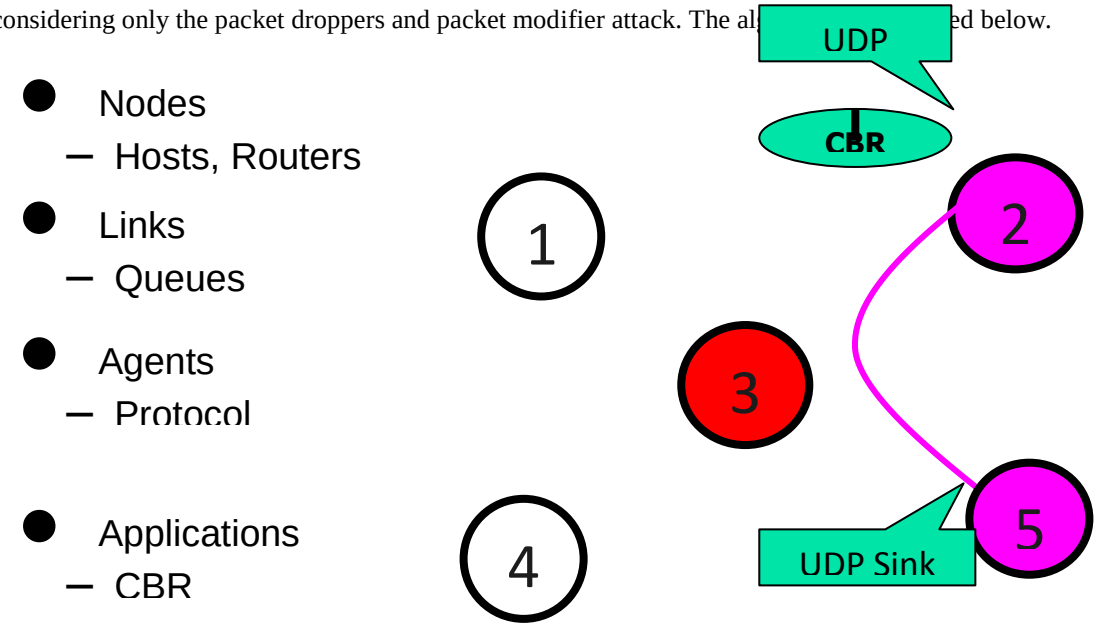


Figure 1: NS Communication Model

4.1.1 Node Categorization Algorithm

1: Input: Tree T, with each node u marked by "þ" or "_,"
and its dropping ratio du.
2: for each leaf node u in T do
3: v u's parent;
4: while u is not the Sink do
5: if u:mark =''+'' then
6: if v:mark = ''-'' then
7: b ← v;
8: repeat
9: e ← v;
10: v ← v's parents node;
11: until v:mark = ''+'' or v is Sink
12: Set nodes from b to e as bad for sure;
13: else
14: if v is Sink then

15: Set u as bad for sure;

16: if v.mark = ‘‘+’’ then

17: if v is not bad for sure then

18: Set u and v as suspiciously bad;

19: else

20: if dv - du > θ then

21: Set v as bad for sure;

22: else if du - dv > θ then

23: Set u and v as suspiciously bad;

24: u ← v, v ← v’s parents node

4.1.2 The Global Ranking-Based Approach

1: Sort all suspicious nodes into queue Q according to the descending order of their accused account values.

4.1.3 Algorithm for Trust-Based Intrusion Detection

Our trust-based IDS algorithm is based on selecting a system minimum trust threshold, T^{th}, below which a node is considered compromised and needs to be excluded from sensor reading and routing duties. The underlying principle is that a compromised node will exhibit several social and QoS trust behaviors, i.e., low intimacy and low honesty (for social trust) as well as low energy and low unselfishness (for QoS trust), thus exposing itself as a compromised node under hierarchical trust evaluation. A CH performs CH-to-SN trust evaluation toward node j after receiving T_{ij} (t) values from all SNs in the cluster. More specifically a CH, c, when evaluating a SN, j, will compute node j’^{s} trust value, T_{cj} (t), by Equation 4. CH c will announce node j as compromised if T_{cj} (t) is less than T^{th}; otherwise, node j is not compromised.

4.1.4 DPDSN: Detection Of Packet-Dropping Attacks For WSN.

DPDSN stands for Detection of Packet Dropping attacks for wireless Sensor Networks, uses the observation that alternate routing paths are readily available in WSNs, which are typically dense. DPDSN monitors paths and detects whether any node on a path drops packets. Once we detect such an event, we switch to an alternate path for communication. We always keep an alternate path ready to minimize the switching delay. The cost of finding an alternate path is minimized by having it embedded in route discovery of source-initiated and receiver-initiated routing protocols.

4.1.5 Secure Multipath Routing For Mobile Ad -Hoc Networks

A novel on-demand, multipath routing protocol, secure against a bounded number of colluding malicious nodes, the Secure Multipath Routing protocol (SecMR). SecMR discovers the complete set of the existing non-cyclic, node-disjoint paths between a source and a target node, for a given maximum hop distance.

4.1.6 Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks

In distributed probing technique, every node in the network will probe the other nodes periodically to detect if any of them fail to perform the forwarding function. Subsequently, node state information can be utilized by the routing protocol to bypass those malicious nodes. In a moderately changing network, the probing technique can detect most of the malicious nodes with a relatively low false positive rate. The packet delivery rate in the network can also be increased accordingly.

4.1.7 A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks

A resilient packet-forwarding scheme using Neighbor Watch System (NWS). specifically designed for hop-by-hop reliable delivery in face of malicious nodes that drop relaying packets, as well as faulty nodes that fail to relay packets. Our scheme basically employs single-path data forwarding, which consumes less power than multipath schemes. As the packet is forwarded along the single-path toward the base station, our scheme, however, converts into multipath data forwarding at the location where NWS detects relaying nodes' misbehavior.

4.2 A Survey of Trust Management in Mobile Ad-Hoc Networks

4.2.1 Trust Prediction

The prediction of trust between nodes is an emerging strand of research in the area where unknown trust values exist can be calculated using information of the past and present behavior of nodes.

4.2.2 Trust Aggregation

As trust is propagated through the network, multiple accounts of trust for a single node will be received by a node. The different values of trust will be required to be aggregated in order to calculate a final value of trust.

4.2.3 Discovery and Computations of Trust

In distributed ad-hoc networks, trust levels are devised from the analysis of collected data from observations for specific actions. This could include packet routing, where a node might observe the routing behavior of another node. It could log that a particular node forwards some packets as normal, and then drops other packets. It could receive this through direct neighbor sensing and calculate trust from direct experience. Trust between immediate neighboring nodes is known as Direct Trust and is required for cases where a trust relationship is formed between two nodes without previous interactions.

4.2.4 Hybrid Trust and Reputation Management for Sensor Networks

A trust management model that can uniformly support the needs of nodes with highly diverse network roles and capabilities, by exploiting the pre-deployment knowledge on the network topology and the information flows, and by allowing for flexibility in the trust establishment process. The model is hybrid, combining aspects from certificate-based and behavior-based approaches on trust establishment on common evaluation processes and metrics. It enables controlled trust evolution based on network pre-configuration, and controlled trust revocation through the propagation of behavior evaluation results made available by supervision networks.

4.2.5 Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks

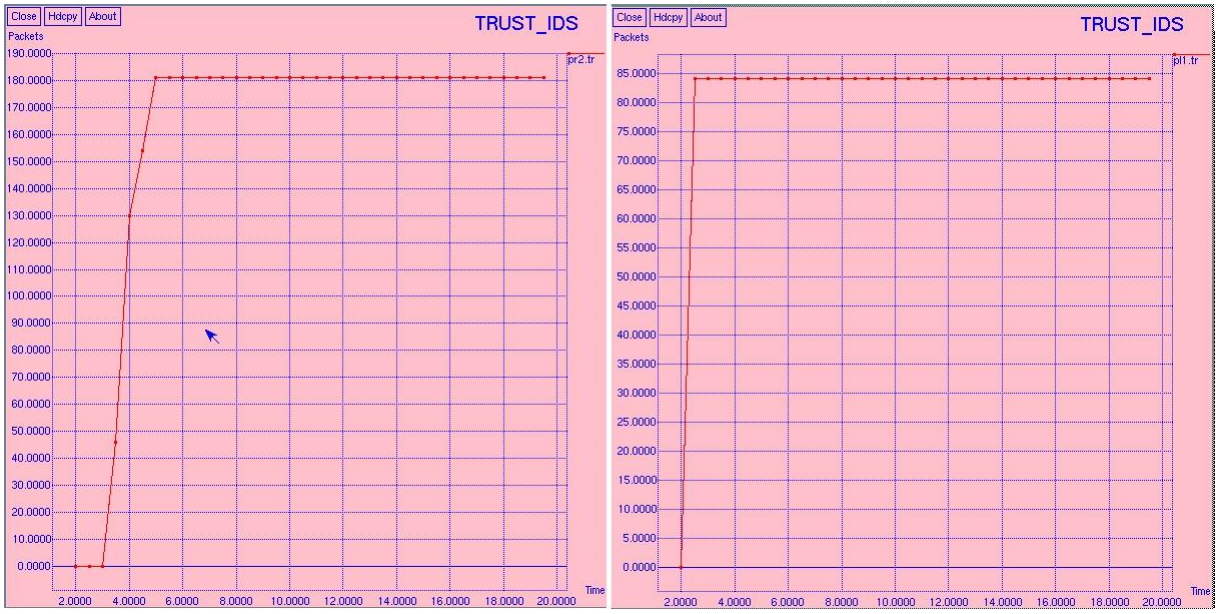
A new lightweight group-based trust management scheme (GTMS) for wireless sensor networks, which employs clustering. Our approach reduces the cost of trust evaluation. Also, theoretical as well as simulation results show that our scheme demands less memory, energy, and communication overheads as compared to the current state-of-the-art trust management schemes and it is more suitable for large-scale sensor networks. Furthermore, GTMS also enables us to detect and prevent malicious, selfish, and faulty nodes.

4.2.6 Trust Management Architecture for Hierarchical Wireless Sensor Networks

Security and trust are fundamental challenges when it comes to the deployment of large wireless sensor networks. So, they propose a novel hierarchical trust management scheme that minimizes communication and

storage overheads. Our scheme takes into account direct and indirect (group) trust in trust evaluation as well as the energy associated with sensor nodes in service selection. It also considers the dynamic aspect of trust by introducing a trust varying function which could give greater weight to the most recently obtained trust values in the trust calculation.

V. PACKET TRANSMITTED



VI. PERFORMANCE ANALYSIS

VII. CONCLUSION

In our project, we propose a unified solution, which serves as the front line in defending against all types of security threats. Specifically, we further proposed a proactive data security framework (PDSF) to identify compromised and faulty nodes proactively and prohibit them from participating network activities in a dynamic manner. PDSF consists of two key modules, misbehavior characterization & monitoring, and trust management. The former characterizes different types of misbehavior in WSNs and defines a set of monitoring criteria. And the latter develops a trust management model, which adapts itself to the resource constrained and application specific nature of the WSNs.

REFERENCES

[1]. High Speed Networks & Internets Performance and Quality of service, William Stallings, Second Edition, Pearson Education.
[2]. Cryptography and Network Security (principles & practices),William Stallings, prentice hall of india-2008.
[3]. Computer Networks (protocols, standards, interfaces), uyless black, Prentice Hall of India-2006.
[4]. Modern Cryptography (theory & practice), wenbo mao, first edition, pearson education-2006.
[5]. Computer networks "A system approach" larry L.peteson and Bruce S.Davie, Fourth edition, Morgan Kaufmann publishers.
[6]. Wireless communication (principles & practice), Theodore S.Rappaport, Second Edition, Pearson hall of india-2008.
[7]. TCP/IP Protocol suite, Behrouz A.Forouzan, Fourth edition, Tata McGraw Hill Edition.
[8]. Design of a role based trust management framework by John C.Mitchell, William H.Winsborough.
[9]. A Proactive Data Security Framework for Mission-Critical Wireless Sensor Networks by Kui Ren, Wenjing Lou, and Patrick J. Moran.
[10]. www.isi.edu/nsnam/ns
[11]. www.winlab.rutgers.edu
[12]. www.Citeseerx.ist.psu.edu