Security Fundamentals & Measures on DDoS Attack in wireless sensor network: A Survey

Prof. Sunny G. Gandhi[1], Prof. Palash M. Gourshettiwar[2]
[1]*Asst. Prof. Dept. of Information Tech., D.M.I.E.T.R Sawangi(M), Wardha*
[2]*Asst. Prof. Dept. of Computer Tech. K.D.K.C.E Nagpur*

Abstract- As the serious damage caused by DDoS attacks increases, the rapid detection and the proper response mechanisms are urgent. Existing security mechanisms do not provide effective defense against these attacks, or the defense capability of some mechanisms is only limited to specific DDoS attacks. It is necessary to analyze the fundamental features of DDoS attacks because these attacks can easily vary the used port/protocol, or operation method. In this paper, we propose a combined data mining approach for modeling the traffic pattern of normal and diverse attacks. This approach uses the automatic feature selection mechanism for selecting the important attributes. And the classifier is built with the theoretically selected attribute through the neural network. And then, our experimental results show that our approach can provide the best performance on the real network, in comparison with that by heuristic feature selection and any other single data mining approaches.

I. INTRODUCTION

Security

Network security is one of the most pressing concerns in all wireless networks, including wireless sensor networks. In this section, we briefly introduce the security problem and explain some of the specifics of wireless sensor networks.

Fundamentals

Network designers have to be aware of and decide about suitable mechanisms to implement one or more of the following general **security goals.**

Confidentiality Information should only be revealed to authorized entities; any other entity should not be able to discover the information from eavesdropping or from reading memories.

Data integrity The receiver of information wants to be sure that it is not modified in transit, either intentionally or by accident. To distinguish unmodified "wanted" information from unmodified bogus information, the originator must be identifiable uniquely.

Accountability The entity requesting a service, triggering an action, or sending a packet must be uniquely identifiable.

Availability Legitimate entities should be able to access a certain service/information and to enjoy proper operation.

Controlled access A service or information access should only be granted to authorized entities. Any security analysis must start with stating the desired security goals, followed by an assessment of the possible risks or security threats posed by an attacker. Some common threats are eavesdropping, masquerading (i.e. pretending to have another entity's identity), authorization violation (using services without being allowed to use them), provoking loss or modification of information, forgery (i.e. creating new information), repudiation, and sabotage.

When considering networking, some of the common attacks are eavesdropping as a purely passive attack, and insertion, deletion, or replaying of packets as an active attack. Attacks can be placed on all the layers of a given protocol stack.

Many countermeasures have been developed against these threats. These mechanisms frequently rely on symmetric or asymmetric **cryptographic algorithms**. These algorithms can be used to encrypt data packets, to sign these with almost unique hash/cryptographic check values, or to create certificates. Cryptographic algorithms essentially work by applying certain operations on combinations of the user data and specific key values, which optimally are only known to the sender and the receiver of a packet. Distributing these keys to the users and taking care of their lifecycle are essential parts of key management protocols. In practice, key management turns out to be the most complex part of security protocols; the raw encryption and decryption procedures are small but important building blocks.

Security considerations in wireless sensor networks Can security measures and cryptographic protocols in wireless sensor networks be considered in the same way as for other types of networks? There is some consensus that the answer seems to be "no", for the following reasons:

• The network infrastructure of a WSN is made up of small, cheap nodes spread over a possibly hostile area. Unlike other types of networks, it is often impossible to prevent the sensor nodes from being physically accessed by attackers. This is also referred to as node capture. It is reasonable to assume that an attacker can achieve full control over a captured node, that is he can read its memory or influence the operation of the node software. Special secure memory devices would be

needed to prevent the attacker from reading the memory; however, these will only rarely be present in cheap sensor nodes.

• The constraints regarding memory and computational capabilities are a serious obstacle for implementing cryptographic algorithms. Especially asymmetric key cryptography is considered too heavyweight for small processors, let alone the key management involved. The usage of several cryptographic block ciphers in sensor networks has been investigated in reference.

• When in-network processing is to be performed, intermediate nodes need to access and modify the information contained in packets; hence, a larger number of parties is involved in end-to-end information transfers.

• The finite energy budget of sensor nodes opens up a particularly attractive line of attacks: to force victim sensor nodes to exhaust their energy budget quickly and to die.

An additional challenge pointed out is that attackers can have much more energy at their disposal than the sensor nodes. All security measures carried out by a sensor node require extra energy and stressing the node by attacks can cause premature depletion. This amounts to one particular kind of a denial-of-service attack (DoS). In the following, some of these DoS attacks are briefly described.

II. DENIAL-OF-SERVICE ATTACKS

Consider a number of different denial-of-service attacks in sensor networks, working at different levels. Denial-of-service attacks in general can try to(i) disable services, or (ii) to deplete service providers, for example, by overusing the service. To disable a sensor network's service, an attacker might simply destroy nodes. Although sensor networks have some resilience to node failures, the attacker can distort the network by destroying a large number of nodes or by focusing on especially important nodes, for example, sensor nodes in the vicinity of sinks that are needed for forwarding. In the following, however, we discuss protocol-related attacks.

Physical-layer and link-layer attacks With physical-layer jamming, an attacker simply distorts radio communication. One way to achieve this is to place attacker nodes somewhere into the network and let them continuously send radio signals in the sensor network's frequency band. Especially effective is such an attack when the attacker nodes are close to sink nodes, effectively reducing a user's ability to control the network or to acquire data from it. A single attacker node can distort many neighbors at once and, by strategical placement of a number of attacker nodes, the whole sensor network can be disabled.

One possible countermeasure is the use of modulation schemes with some robustness against interference, A second possible countermeasure is that the uncompromised

sensor nodes reduce their duty cycle upon detecting such an attack. If the attacker has itself only a finite energy budget, it can persevere only for a limited time. A third countermeasure can be taken by routing protocols: If the attacker jams only a limited area, packets may be routed around. In protocols like directed diffusion, frequent interest dissemination can find working routes. Finally, sensor nodes with different physical layers can switch between these

A cleverer attacker can take knowledge about the protocols into account to save energy, giving rise to **link-layer jamming**. Especially, the MAC protocol is a good candidate. Let us consider, for example, protocols based on exchange of RTS/CTS packets like PAMAS. Whenever an attacker node *a* receives an RTS packet issued by some node *x*, it can answer with a jamming signal, interfering with any CTS packet sent to *x*. As a consequence, *x* has no transmit opportunity, backs off and tries again later with another RTS packet. According to Wood and Stankovic no effective countermeasure against such an attack exists. The attacker might exploit the MAC protocol further to save energy. For example, in S-MAC the attacker can adapt its activity periods to the schedules of its neighbors.

Another ugly attack exploits MAC protocols using immediate acknowledgments and retransmissions.

Upon receiving a data frame from node *x*, the attacker node can jam the acknowledgement frame destined to *x*. This causes *x* to back off, retransmit the same packet and to waste energy.

Another way of depleting a node *x* is to continuously send RTS packets to this node, causing him to answer with CTS packets.

III. NETWORK-LAYER ATTACKS

Several types of attacks can be executed on the network layer. First, attacker nodes can behave similar to normal nodes; specifically, they can participate in routing protocols or dissemination of interests with the goal of directing routes to itself and to drop packets later on. This attack is called **black hole** attack. For example, in distance-vector protocols, the attacker can pretend to have particularly good routes to the sink. Dropping of packets destroys information, and furthermore, the forged route advertisements attract lots of traffic around the attacker, causing increased congestion levels and contention.

In a similar kind of attack, so-called **misdirections**, the adversary creates wrong routes, for example, by sending wrong route advertisement packets or by falsely answering route request packets. A wrong route can, for example, contain a loop and cause waste of energy. Another possible effect is that traffic does not reach the intended sink nodes. Instead of creating wrong routes, an adversary can also cause creation of unnecessary routes, for example, by issuing route lookup requests. All nodes participating in route selection waste their energy.

Even without actively trying to be included as a forwarder into routes, an attacker node can drop other nodes' packets and forward only its own packets. Such an attack is called **neglect and greed**. The attacker node can drop packets in a random fashion or all of them. Routing or data dissemination protocols that cache routes (like DSR or directed diffusion) are vulnerable to this attack. The attacker node participates in route setup and distorts, later on, the forwarding of data packets. When this behavior has been detected, the network may set up alternate routes or a source node can send multiple copies of a packet over node-disjoint routes from the beginning.

All these attacks have their source in adversary nodes participating in routing protocols. To prevent this, authentication and/or authorization mechanisms are needed to restrict routing protocols only to trustworthy nodes. Protocols for this purpose are beyond the scope of this chapter.

An attack called **homing** seeks to determine the geographic locations of certain important nodes in the network, for example cluster head nodes. This information can be obtained from eavesdropping location-centric protocols. Once this information has been determined, the adversary can direct other attacks to these nodes. Clearly, a good way to prevent this attack is encryption of location information.

Transport layer and application attacks

If the transport layer uses explicit connections between identifiable nodes, either end of the connection needs to maintain some form of connection control block (CCB). Similar to TCP syn flood attacks, an attacker can issue a large number of connection setup requests and cause exhaustion of memory at the end nodes because of large numbers of unneeded CCBs.

Another kind of attack is **desynchronization**, which can be applied to transport protocols resting on sequence numbers. By issuing forged packets with wrong sequence numbers, the attacker can cause wasteful retransmissions or even cause the participants to end the connection.

In sensor networks deployed to detect certain environmental events, an attacker node can generate sensor data indicating this event, causing nodes in the vicinity or even the whole network to wake up and to start various activities. Possible countermeasures can be developed starting from outlier detection techniques.

IV. REFERENCES

[1] Mihui Kim, et al.: A Combined Data Mining Approach for DDoS Attack Detection. Proc. of ICOIN (2004) 1365-1374

[2] Wenke Lee, Salvatore J. Stolfo: Data Mining Approaches for Intrusion Detection. Proc. of the 7th USENIX Security Symposium (1998) 79-94

[3] Hyunjung Na, et al.: Distributed Denial of Service Attack Detection using Netflow Traffic. Proc. of the Korea Information Processing Society (2003)

[4] LI Aijun, LIU Yunhui and LUO Siwei: Mapping a Decision Tree for Classification into a Neural Network. Proc. of the 6th International Conference on Computational Intelligence & Natural Computing (2003)