TRUST AWARE ROUTING FRAMEWORK FOR WSN

Mrs.R.Radhika[1]
II yr ME CSE
Srinivasan Engineering College.
Perambalur
Krishna.radhika055@gmail.com

Mr. V.Senthil Murugan [2], Asst.Prof,
Department of CSE,
Srinivasan Engineering College.
Perambalur

Abstract- Wireless sensor networks (WSNs) are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities, the multi-hop routing of WSNs often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

To focus on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attacks, sinkhole attacks and Sybil attacks.

In this project is aimed to protect WSNs from the harmful attacks exploiting the replay of routing information, so designed and implemented a robust trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks. Based on the unique characteristics of resource-constrained WSNs, the design of TARF centers on trustworthiness and energy efficiency.
Keywords: WSN, wormhole attack, sinkhole attack

1.INTRODUCTION

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high-level analysis. Communication between two hosts using a network may be encrypted to maintain privacy.

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, a hacker begins by exploiting vulnerability in one computer system and making it

the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple sometimes thousands of compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service.

While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack the final target and as well the systems controlled by the intruder. Although the owners of co-opted computers are typically unaware that their computers have been compromised, they are nevertheless likely to suffer degradation of service and malfunction. Both owners and users of targeted sites are affected by a denial of service. DDoS attacks can also create more widespread disruption.

A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets not spam, viruses, or worms as the biggest threat to Internet security.

It is an extraordinary challenge to traceback the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying normal service or degrading of the quality of services. It has been a major threat to the individual attacks are more strong and sophisticated.

IP traceback means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, may not be able to find the actual hackers at present. In fact, IP traceback schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the Internet.

A number of IP traceback approaches have been suggested to identify attackers and there are two major methods for IP traceback, the probabilistic packet marking and the deterministic packet marking . Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where the defender has the authority to manage.

However, this kind of ISP networks is generally quite small, and cannot traceback to the attack sources located out of the ISP network. The DPM strategy requires all the Internet routers to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability is a huge problem. Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers. Therefore, it is infeasible in practice at present.

In the previous work on DDoS attack detection, the packet number distributions of packet flows are compared, which are out of the control of attackers once the attack is launched, and is found that the similarity of attack flows is much higher than the similarity among legitimate flows, e.g., flash crowds.

Entropy rate, the entropy growth rate as the length of a stochastic sequence increases, was employed to find the similarity between two flows on the entropy growth pattern, and relative entropy, an abstract distance between two probabilistic mass distributions, was taken to measure the instant difference between two flows.

2.PROBLEM STATEMENT

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity; the

malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets, which is known as a wormhole attack.

A node in a WSN relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. It may drop packets received, forward packets to another node not supposed to be in the routing path, or form a transmission loop through which packets are passed among a few malicious nodes infinitely.

Sinkhole attacks can be launched after stealing a valid identity, in which a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole." This same technique can be employed to conduct another strong form of attack Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks

3.PROPOSED WORK

To protect WSNs from the harmful attacks exploiting the replay of routing information, designed and implemented a robust trust-aware routing framework, TARF, to secure routing solutions in wireless sensor networks.Based on the unique characteristics of resource-constrained WSNs, the design of TARF centers on trustworthiness and energy efficiency. TARF requires neither tight time synchronization nor known geographic information.TARF proves resilient under various attacks exploiting the replay of routing information, which is not achieved by previous security protocols. Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition, TARF demonstrates steady improvement in network performance. Implemented a ready-to-use TARF module with low overhead, which as demonstrated can be integrated into existing routing protocols with ease.

This is mainly based on the topology construction process for that a TARF framework has been implemented for that the TARF should be updated with the existing protocol. To implement this project JAVA has been used to create the server,client and intermediate node model and the Java coding is utilized for policy creation(protocol) too. The IDE used in this project is netbeans 6.9.1 and dll have been incorporated to achieve the network model.

In network model the client,server, intermediate node has been generated. Here the security has been created by assigning the trust manager and energy watcher component. The purpose of trust manager and energy watcher has been explained as follows.

3.1 TECHNIQUES USED

TARF secures the multihop routing in WSNs against intruders misdirecting the multihop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput.

Energy Watcher

A node N's EnergyWatcher computes the energy cost ENb for its neighbor b in N's neighborhood table and how N decides its own energy cost EN. Before going further, ENb mentioned is the average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next-hop node being responsible for the remaining route. Here, one-hop retransmission may occur until the acknowledgment is received or the number of retransmissions reaches a certain threshold.

The cost caused by onehop retransmissions should be included when computing ENb. Suppose N decides that A

should be its next-hop node after comparing energy cost and trust level.

Trust Manager

Once a loop has been detected by N for a few times so that the trust level of the next-hop node is too low, N will change its next-hop selection, thus that loop is broken. Though N cannot tell which node should be held responsible for the occurrence of a loop, degrading its next-hop node's trust level gradually leads to the breaking of the loop. On the other hand, to detect the traffic misdirection by nodes exploiting the replay of routing information, TrustManager on N compares N's stored table of <node id of a source node, forwarded sequence interval [a, b] with a significant length> recorded in last period with the broadcast messages from the base station about data delivery.

First introduce several necessary notions. For a node N, a neighbor (neighboring node)of N is a node that is reachable from N with one-hop wireless transmission. **Trust level**: For a node N, the trust level of a neighbor is a decimal number in [0, 1], representing N's opinion of that neighbor's level of trustworthiness. Specifically, the trust level of the neighbor is N's estimation of the probability that this neighbor correctly delivers data received to the base station. That trust level is denoted as T . Energy cost for a node N, the energy cost of a neighbor is the average energy cost to successfully deliver a unitsized data packet with this neighbor as its next-hop node, from N to the base station. That energy cost is denoted as E .

TrustManager is responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about data delivery.

Energy Watcher is responsible for recording the energy cost each known neighbor, based on N's observation of one hop transmission to reach its neighbors and the energy cost report from those neighbors.

TARF implementation can be integrated into the exiting protocols with the least effort, incorporated TARF into a collection tree routing protocol (CTP) .CTP is used for transferring data from one or more sensors to one or more root nodes. The CTP protocol is efficient, robust, and reliable in a network with highly dynamic link topology. It quantifies link quality estimation in order to choose a next-hop nodes

4.SIMULATION WORK AND RESULTS

TARF secures the multihop routing in WSNs against intruders misdirecting the multihop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy efficient, highly scalable, and well adaptable. Before introducing the detailed design,first introduce several necessary notions here.

i) Neighbor node construction-A neighbor node is constructed by one hop transmission phase.

ii) Trust Level-The trust level will be initially distributed at neutral value of 0.5 to each intermediate node the trust level will be upgraded and degraded based upon the response of the broadcasting message of the basestation.

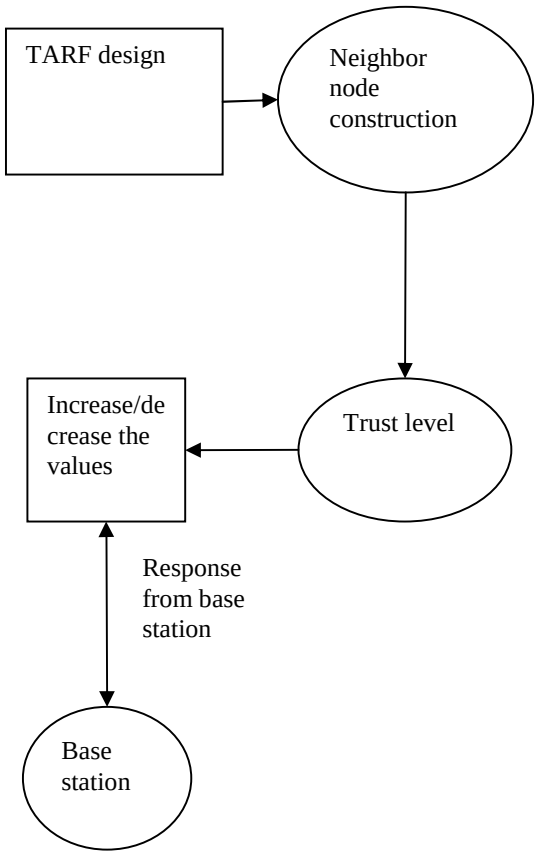

Figure 4.4 Flow Chart for TARF Model Construction

This figure 4.4. describes the design of TARF Model.It also describes the trust level and construction of neighbour node.

4.4.2 Routing Component Analysis

The base station broadcasts a message about data delivery during last period to the whole network consisting of a few contiguous packets (one packet may not hold all the information). Each such packet has a field to indicate how many packets are remaining to
complete the broadcast of the current message. The completion of the base station broadcast triggers the exchange of energy report in this new period. Whenever a node receives such a broadcast message from the base station, it knows that the most recent period has ended and a new period has just started. No tight time synchronization is required for a node to keep track of the beginning or ending of a period.

i) Energy Watcher

The EnergyWatcher on a node monitors energy consumption of one-hop transmission to its neighbors and processes energy cost reports from those neighbors to maintain energy cost entries in its neighborhood table.

ii) Trust Manager

TrustManager also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighborhood table.

4.4.3. Route Discovery Phase

Each node N relies on its neighborhood table to select an optimal route, considering both energy consumption and reliability. TARF makes good efforts in excluding those nodes that misdirect traffic by exploiting the replay of routing information.

For a node N to select a route for delivering data to the base station, N will select an optimal next-hop node from its neighbors based on trust level and energy cost and forward the data to the chosen next-hop node immediately. The neighbors with trust levels below a certain threshold will be excluded from being considered as candidates. Among the remaining known neighbors, N will select its next-hop node through evaluating each neighbor.

4.4.4 Threat Model

In major issues the 3 kinds of attacks will be hosted in the networking wormhole, sinkhole and Sybil attacks . Tarf was incorporated with the existing protocol to improve the efficiency of the attack detection. The algorithm has been enhanced to overcome the DOS attacks. This figure 4.7 describes the Threat model and also identifies the attacks.

5. CONCLUSION

The new paradigm of the ad hoc network presents new challenges on security. The existing solutions cannot solve the security issues for the ad hoc networks. TARF aims to protect Wireless Sensor Networks from harmful attacks such as Sinkhole attack, Wormhole attack and Sybil attack. TARF focuses on Trustworthy and Energy Efficiency to secure multihop routing in Wireless Sensor Network. It is achieved by maintaining neighborhood table. The modules for the proposed system has been designed and the implementation has been finished.

Our main contributions are listed as follows:

1. Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.
2. The resilience and scalability of TARF are proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

REFERENCES

[1]Bai .L, Ferrese .F, Ploskina .K, and Biswas .S, "Performance Analysis of Mobile Agent-Based Wireless Sensor Network," Proc. Eighth Int'l Conf. Reliability, Maintainability and Safety (ICRMS '09), pp. 16-19, 2009.

[2]Jain .M and Kandwal .H, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," Proc. Int'l Conf. Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555-558, 2009.

[3]Karlof .C and Wagner .D, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

[4]Krontiris .I, Giannetsos .T, and Dimitriou .T, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side," Proc. IEEE Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WIMOB '08), pp. 526-531, 2008.

[5]Newsome .J, Shi .E, Song .D, and Perrig .A, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Conf. Information Processing in Sensor Networks (IPSN '04), Apr. 2004.

[6]Xue .W, Aiguo .J, and Sheng .W, "Mobile Agent Based Moving Target Methods in Wireless Sensor Networks," Proc. IEEE Int'l Symp. Comm. and Information Technology (ISCIT '05), vol. 1, pp. 22-26, 2005..

[7]Yan .Z, Zhang .P, and Virtanen .T, "Trust Evaluation Based Security Solution in Ad Hoc Networks," Proc. Seventh Nordic Workshop Secure IT Systems, 2003.

[8]Zhan .G and Shi .W ,"Design and Implementation of TARF for WSNs",in Preceeding of IEEE Transactions on Dependable and Secure Computing,March/April 2012.

[9]Zhan .G, Shi .W, and Deng .J, "Tarf: A Trust-Aware Routing Framework for Wireless Sensor Networks," Proc. Seventh European Conf. Wireless Sensor Networks (EWSN '10), 2010.

[10] Zhang .L, Wang .Q, and Shu .X, "A Mobile-Agent-Based Middleware for Wireless Sensor Networks Data Fusion," Proc. Instrumentation and Measurement Technology Conf. (I2MTC '09), pp. 378-383, 2009.

[11] Zhao .F and Guibas .L, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004.