Secure Smart Grid Network

Priti V. Jasud, A. S. Dhone, S. C. Sakure

Abstract: The Smart Grid is formed by many sub-networks such as the Home Area Network (HAN), t which are at risk and can be attacked remotely. A Smart grid designing a mutual authentication scheme and a key management protocol. This paper proposes an efficient scheme that mutually authenticates a smart grid. In this paper we analyzed three cases first we show the normal execution then execution along with attackers. Using mutual authentication we overcome attacks. A number of anonymous routing schemes have been proposed for grid networks in recent years, and they provide different level of privacy protection at different cost. First, an anonymous key establishment process is performed to construct secret session keys. By using NS-2 the performance analysis such as energy, bandwidth etc., are simulated. Here we find the attacks.

Keywords - Privacy, Public key, smart grid (SG) mutual authentication, and Routing.

I. INTRODUCTION

The Smart Grid is designed to provide the security in which has gained substantial attention in the research community [1]. SG is a combination of different systems and subsystems and is vulnerable various attack that may cause different levels of harms to the devices and even to the society at large [2]. An important problem which is associated with smart grid is the problem of security and privacy. Privacy protection of smart grid network is more demanding than that of wired networks due to the open nature and mobility of wireless media. In contrast, the attacker only needs an appropriate transceiver to receive wireless signal without being detected. In wired networks, devices like desktops are always static and do not move from one place to another. The aim of the Centre is to develop innovative, reliable and quality solutions to provide both utilities and policy makers with technology options to deliver economical and sustainable energy to customers. The Key management is one of the important security requirements to achieve data confidentiality and integrity in smart grid system. The Smart Grid is designed to provide consumers with reliable, efficient, and safe electric energy. Security in the Smart Grid is not only important to securing the new communications and systems on the Internet, but also to ensuring safety and reliability for the critical utility of power.

Manuscript Received on January 2015.

Priti V. Jasud, Asst. Prof., Department of Computer Technology, KDK College of Engineering, Nagpur, India.

A. S. Dhone, Asst. Prof., Department of Computer Technology, KDK College of Engineering, Nagpur, India.

S. C. Sakure, Asst. Prof., Department of Computer Technology, KDK College of Engineering, Nagpur, India.

Providing an authentication scheme and providing key management protocols are the required first steps of designing and implementing system security in SG [3]. This enables private communications between users while making it harder for adversaries to focus their attacks. A solution that provides stronger anonymity properties while also solving some of the efficiency problems.

II. RELATED RESEARCH WORK

In this section, we introduce the mechanism for detecting the wormhole attacks. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. If a node can receive a message from a node at time , then node could instead have received a message from node at the time will implement the watchdog. It maintain a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when forwards a packet from to with the help of , can overhear transmission and capable of verifying that has attempted to pass the packet towards . But this approach has some limitations and it is not detect the misbehaving node during ambiguous collisions, receiver collisions, false misbehavior and collusion. The approach is used directional antenna to detect and prevent the wormhole attack. The technique is assumed that nodes maintain accurate sets of their neighbors. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are ignored. It does not require even the aggregation of any special information, since it uses routing data that is already available to a node the main idea behind this approach resides in the fact that the relative frequency of any link that is part of the wormhole tunnel, will be much higher than other normal links. To estimate the direction of received signal and angle of arrival of a signal it uses directional antennas. This scheme works only if two nodes are communicating with each other, they receive signal at opposite angle. But this scheme is failed only if the attacker placed wormholes residing between two directional antennas.

III. PROPOSED WORK

We have performed the simulation of the proposed scheme in practical efficiency of the scheme; the physical parameter considerations are same as taken
in mathematical modeling.

Step1. Randomly Generate a Number in between 0 to maximum number of nodes.

Step2. Make the Node with same number as transmitter node.

Step3. Generate the Route from selected transmitting node to any destination node with specified average route length.
Step4. Send packet According to selected destination and start timer to count hops and delay.
Step5. Repeat the process and store routes and their hops and delay.
Step6. Now if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker.
Step7. Now check the delay of all previous routes which involve any on node of the suspicious route. Now the node not encounter previously should be malicious let there are N such nodes.
Step8. In N == 1 then it is the attacker else wait for future sequences which shows deviation and involve only one of N nodes.
Step9. These nodes are black listed by the nodes hence they are not involved in future routes.
Step10. Whole process (from step1 to step9) is repeated until we didn't get the specified goal (goal can be
1. To get complete list of malicious nodes.
2. To run for specified time.
3. To run for specific number of packets etc.

IV. SYSTEM IMPLEMENTATION

In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric crypto. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, Smart grid comprises two phases: anonymous trust establishment and unobservable route discovery.

A. Topology Formation & Anonymous Key establishment

Constructing project design in NS2 should takes place. In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment. Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors.

B. Privacy-Preserving Route Discovery

This phase is a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply. Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node.

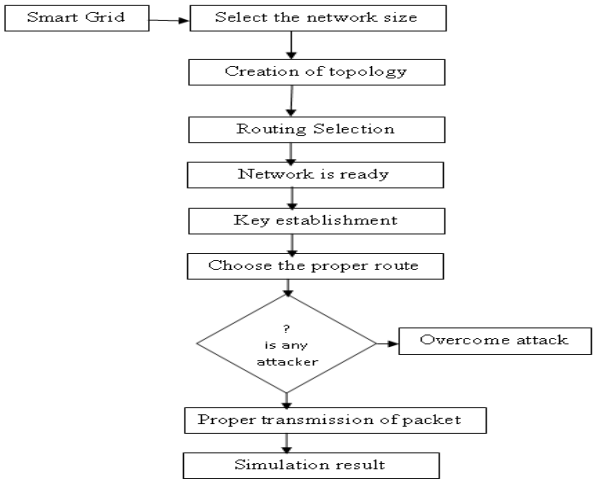

Fig. System Design

V. SIMULATION ANALYSIS AND RESULT

This proposed routing protocol has been implemented by the Network Simulator2 (NS2). The Network Simulator is mainly utilized to implement the routing protocols in the networking research. The Main focus of our analysis is security and privacy. The simulation results are shown below.

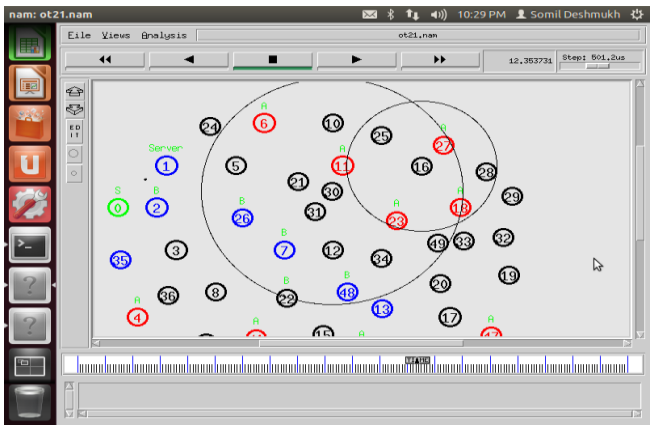

Fig. 3 Topology Formation & Anonymous Key Establishment

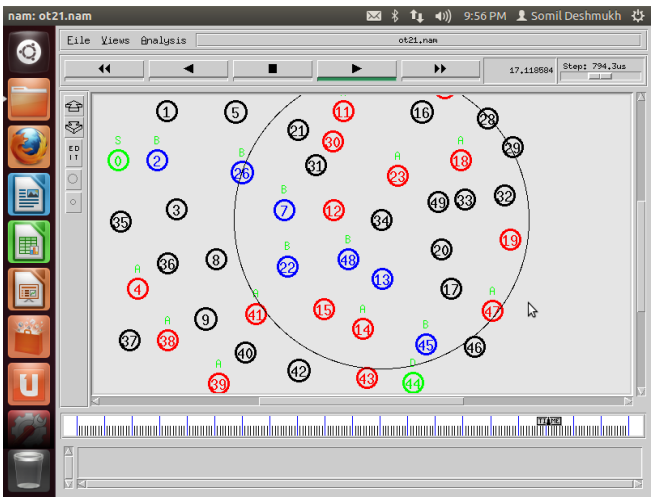

Fig. Privacy- Preserving Route Discovery

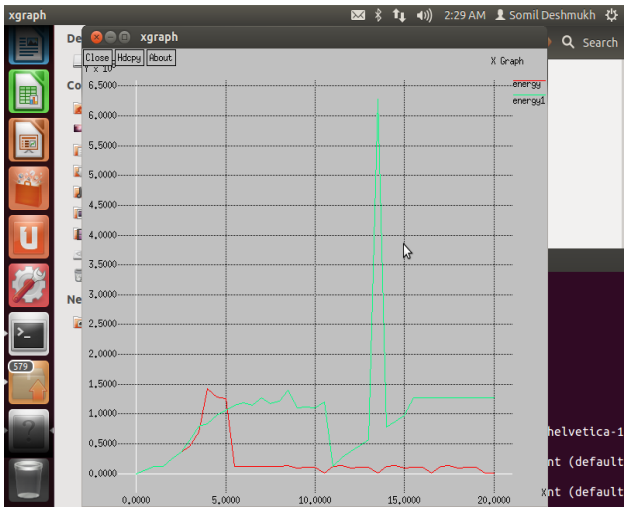

Fig. Maximum throughput

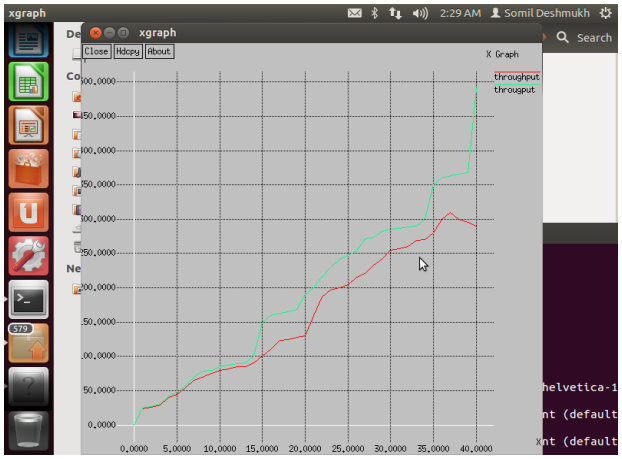

Fig. Minimum energy

VI. SMART GRID APPLICATION

i) Advanced metering infrastructure (AMI):
Establish two-way communications between advanced meters and utility business systems.

ii) Cyber security:
Ensure the confidentiality, integrity and availability of the electronic information.

iii) Demand response and consumer energy efficiency:
Provide mechanisms and incentives for customers to cut energy use during times of peak demand.

iv) Distribution grid management:
Maximize the performance of feeders, transformers and other components of distribution systems.

v) Electric transportation:
Enable large-scale integration of plug-in electric vehicles.

vi) Energy storage:
Provide the means to store energy.

vii)Network communications:
Identify performance metrics and core operational requirements of various Smart Grid applications.

viii) Wide-area situational awareness:
Monitoring and display of power-system components over large geographic areas in near real time to optimize management of grid components and performance and respond to problems before disruptions arise.

VII. CONCULSION

In this phase, every node in the Smart grid network communicates with its direct neighbors within its radio range for anonymous key establishment. Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. This method is Topology Formation & Anonymous Key establishment. And also a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply. Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node. This method is Privacy-Preserving Route Discovery.

FUTURE WORK

After the source node S successfully finds out a route to the destination source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of pseudonyms and keys. The proposed method should focus on full and full privacy preserved routing in mobile networks. The various attacks are overcome. Only security has been improved.

REFERENCE

1. Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, “Smart grid communications: Overview of research challenges, solutions, and standardization activities,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 21–38,2013.
2. J.Wang and V. Leung, “A survey of technical requirements and Consumer application standards for IP-based smart grid AMI network,” in Proc. ICOIN, 2011, pp. 114–119.
3. H. Nicanfar, P. Jokar, and V. Leung,“Smart grid authentication and key management for unicast and multicast communications, ” in Proc. IEEE PES ISGT, 2011, pp. 1–8.
4. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, “Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” Internet Engineering Task Force, Fremont, CA, USA, 2008.
5. M. Amin, “Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid,” in Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, Jul. 2008, pp. 1–5.
6. A. Metke and R. Ekl, “Security technology for smart grid networks,” Smart Grid, IEEE Transactions on, vol. 1, no. 1, pp. 99 –107, Jun. 2010.
7. Z. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, “Towards secure targeted broadcast in smart grid,” IEEE Commun. Mag., vol. 50, no. 5, pp. 150–156, May 2012 [Online]. Available: http://bbcr.uwaterloo.ca/h8liang/sg/Papesg commx.pdf
8. J. Xia and Y. Wang, “Secure key distribution for the smart grid,” IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.
9. light-weight message authentication scheme for smart grid communications,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675–685, 2011.
10. S. R. Rajagopalan, L. Sankar, S.Mohajer, and H. V. Poor, “Smartmeter privacy: A utility-privacy framework,” Proc. IEEE SmartGridComm, 2011.