Different Security Protocol in Mobile Ad-Hoc Networks: A Review

Sandeep Shivhare[1], Sriram Yadav[2], Madhuvan Dixit[3]

[1]M.Tech (PG Scholar), [2]Associate Professor (Head, PG), [3]Associate Professor

(Department of CSE), MITS, Bhopal

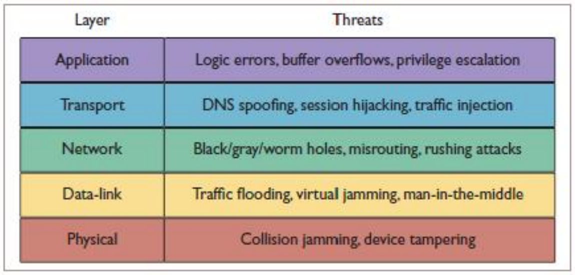
Abstract - Distributed wireless mesh sensor networks (IEEE 802.11s) provide cost-effective communications for deployment in several smart grid areas, such as home area networks (HAN), neighborhood area networks (NAN), and substation/plant-generation local area networks. The traditional wireless network is currently evolving into the smart grid. Smart grid integrates the traditional wireless network with information and communication technologies (ICT). Such integration empowers the computing utilities providers and users, improves the efficiency and the availability of the wireless networks while constantly monitoring, controlling and managing the demands of network users. A smart grid is a huge complex network composed of millions of devices and entities connected with each other. Such a massive network comes with many security concerns and vulnerabilities. In this paper, we survey the latest on smart grid security. We highlight the complexity of the smart grid network and discuss the vulnerabilities specific to this huge heterogeneous network. We discuss then the challenges that exist in securing the smart grid network and how the current security solutions applied for IT networks are not sufficient to secure smart grid networks. We conclude by over viewing the current and needed security solutions for the smart gird.

Keywords - IEEE 802.11s, Smart grid security, information and communications technologies, advanced metering infrastructure, Smart grid, wireless mesh networks.

1. Introduction

The advances in mobile computing and wireless communications, mobile ad hoc networks (MANETs) are becoming more attractive for use in military applications. Supporting security-sensitive applications in hostile environments has become an important research area for MANETs since MANETs introduce various security risks due to their open communication medium, node mobility, lack of centralized security services, and lack of prior security association [3]. In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources. Because the chance of a device in a hostile environment being captured is extremely high, authentication needs to be performed continuously and frequently [2]. User authentication can be performed by using one or more types of validation factors: knowledge factors, possession factors, and biometric factors. Knowledge factors (such as passwords) and possession factors (such as tokens) are very easy to implement but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. Wireless mesh networks (WMNs)

Offer improved utility and lower infrastructure costs than conventional wireless networks because, like mobile ad hoc networks MANETs, they use multi-hop routing. This routing strategy extends the wireless service area and enables the network's self-healing and self-organizing properties. A WMN is distinct from MANETs in that it uses multiple radios and relies on a high-speed back-haul network— itself, often wireless — that optimizes network performance and provides gateways to the wired Internet and other wireless services.



Layer	Threats
Application	Logic errors, buffer overflows, privilege escalation
Transport	DNS spoofing, session hijacking, traffic injection
Network	Black/gray/worm holes, misrouting, rushing attacks
Data-link	Traffic flooding, virtual jamming, man-in-the-middle
Physical	Collision jamming, device tampering

Figure 1: Wireless Security Risks: Security threats are present at all layers of the wireless mesh network stack.

As Figure 1 illustrates, security threats are present at all levels of the protocol stack, so security is a high priority within TGs. The draft amendment builds on the successful security protocols of the base standard and extends them so that they may be used in a WMN environment. In this article, we consider the challenges to WMN security at the data-link or MAC layer and the network layer.

2. Related Work:

Smart Grid Mesh Network Security Using Dynamic Key Distribution with Merkle Tree 4-Way Handshaking (March-2014) [1]: This paper introduces a dynamically updating key distribution strategy to enhance mesh network security against cyber attack. The scheme has been applied to two security protocols known as simultaneous authentication of equals (SAE) and efficient mesh security association (EMSA).

Extensible Authentication Protocol (EAP) and IEEE 802.1x-Tutorial and Empirical Experience [2]: It presents the technical details of the Extensible Authentication Protocol (EAP) and IEEE 802.1x by using WIRE1x, an open-source implementation of IEEE 802.1x client (supplicant) and various EAP-based authentication mechanisms.

A Survey of Wireless Mesh Networking Security Technology and Threats [3]: new challenges with wireless mesh architectures using 802.11, the pending solutions with 802.11s, and the security pitfalls of metro-WiFi networks rekindle many of the original threats and technology maturity issues with ubiquitous wireless access networking.

Security for Smart Distribution Grid by Using Wireless Communication [4]: Connecting equipment, devices and appliances through wireless communication is essential for Smart Distribution Grid (SDG). Mounting suitable wireless communication design and its security measures is extremely important for SDG. The Wireless communication design is proposed for SDG on Wireless Mesh Networks (WMNs). Its bidirectional communication and electricity flow enable both utilities and customer to monitor, forecast and handle energy usages.

High Security for MANETs Using Authentication and Intrusion Detection with Data Fusion [5]: This paper concentrates on the Intrusion Detection and authentication with data fusion in MANET. To overcome the fault in unimodal biometric systems, Multimodal biometrics is set out to work with Intrusion Detection Systems. Each and every device has dimensions and estimation limitations, many devices to be selected and with the help of Dempster-Shafter theory for data fusion observation precision gets increased.

Smart Grid Security: Threats, Vulnerabilities and Solutions [6]: The traditional electrical power grid is currently evolving into the smart grid. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers, improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers.

3. Network Security in Mesh Network:

The conventional WLAN security mechanisms (e.g., such as WPA2/802.11i) provide standardized methods for authentication, access control and encryption between a wireless client and an access point. Since most wide-area mesh solutions strive to retain compatibility with commercial off-the- shelf WLAN client adapters, existing standardized WPA2 mechanisms are commonly retained (e.g., the mesh network “looks like” an access point to the client). However, there are many different types of wireless mesh architectures, where each type of architecture may use a different approach for wireless security. Many approaches for mesh security may be derived from ad-hoc security research, but any future commercial mesh products will standardize security through 802.11s (e.g., will be based primarily on 802.11i security mechanisms).

3.1 Client Access Controls

Wireless mesh infrastructure networks provide access to wireless clients. In most 802.11-based wireless networks, clients are standard wireless LAN stations with no mesh networking capabilities. Some vendors, such as Motorola and Packet Hop offer client mesh solutions, but all Metro-WiFi technologies are intended on providing access to non-mesh capable 802.11 stations. Client access security may vary depending on the type of network: a Metro-WiFi network may use open wireless authentication with a Layer 3 billing service access gateway, while an enterprise/private mesh network will typically use WPA2-compliant wireless access controls.

3.2 Ad-hoc Security and Research

Ad-hoc networks (often called Mobile Ad-Hoc Networks or MANETs) are the evolutionary basis of mesh networking technology that forms the basis of fixed wireless mesh networks. Sharing similar concerns with fixed mesh networks, threat models for ad-hoc networks raised concerns about hackers being able to directly attack the network to delete messages, inject erroneous messages, or impersonate a mesh node. The most prevalent on-demand and link-state routing algorithms do not specify a scheme to protect data or sensitive routing information. This is mainly because any centralized entity could lead to significant vulnerability, where the security solution envisioned for ad-hoc must be based on the principle of distributed trust. There are many different methods within the ad-hoc security research community to address authentication and communication protection in ad-hoc networks. Ad-hoc security research strives to resolve security issues related to trust in a dynamic and arbitrary assembly of nodes, where nodes many originate from different trust realms.

Metro-WiFi deployments will be under administrative and security control of a single network operator, where the fundamental problem is different with no real need for distributed trust. So, why does ad-hoc security matter? While the market momentum with mesh networks revolves around Internet Service Providers (ISP), companies such as PacketHop and Motorola advocate client meshing solutions. Applications for mobile ad-hoc networks are mainly in public safety, where multiple agencies may need to interoperate and communicate at an incident scene. Also, client meshing offers the ability to further extend the reach of the mesh network by providing the ability to hop through client nodes.

In a metro-WiFi mesh deployment, the entire network infrastructure is fixed and under the administrative and security control a single entity where all mesh access points in a mesh network is assumed to belong to single logical administrative domain. Also, the 802.11s standard does not strive to secure mesh between un-trusted devices (e.g., “pure” ad-hoc networks). However, some of the concepts from ad-hoc network security provide insights into key technologies for mesh network security, where a few key ad-hoc security controls are summarized below:

□ Message integrity protection using public/private key security, including transitive trust architectures, between routing peers (SUCV), or message authentication using hash chains to ensure detect tampering of routing information within the network (SEAD);

□ Authentication of routing messages using digital certificates (SAODV); and,

□ Protection by symmetric cryptography using shared secrets or digital signatures.

3.3 Inter-Mesh Access Point Controls

While there are many progressive technologies available through ad-hoc security research, many commercially available mesh networks use a far more simple security model in advance of a mesh security standard. Most existing 802.11-based communication between mesh access points leverages a wireless-distribution system (WDS) mode-of-operation. A conventional (e.g., non-mesh) access point in WDS mode is simple wireless relay between wireless clients and wired access points. Many chipset vendors and mesh equipment providers offer communication protection between nodes using a static key to encrypt WDS links with WEP or AES. With the availability of fully compliant WPA2/802.11i chipsets, separate WPA2 security profiles can be defined for the WDS links (clients will be able to connect to the mesh APs with an alternate security profile – such as without encryption). Thus, there are two primary methods to protect inter-mesh AP communication in advance 802.11s standardization that are based mainly on WPA2/802.11i compliance levels for WDS mode:

□ Static keys configured into the APs at both ends of the WDS link, providing WEP or AES encryptions between mesh nodes.

□ WPA2/802.11i specifies how key handshake works in ad-hoc mode, letting peers derive dynamic encryption keys. This makes it possible to apply the 802.11i four-way key handshake defined for ad-hoc mode to mesh APs connected by WDS. In other words, mesh traffic relayed using WDS modes for inter-mesh AP traffic is secured by WPA2.

3.4 Standardization

In Figure 2, The IEEE is presently working on a standard for mesh networking through the 802.11s working group. The standard will use the WPA2/802.11i security methods to protect the wireless links, where the key principles in 802.11s security is summarized below:

□ Standardization activities for security will focus on inter-AP security controls, where client access uses standard WPA2/802.11i authentication and encryption.

□ Standardization on security between mesh access points is still being finalized within the standard. However, link-by-link security mechanism will be based on 802.11i, with a security architecture based on 802.1X authentication.

□ Mesh APs may have supplicant, authentication and authentication server roles.

□ EAP 4-way handshakes must occur between all mesh routing peers, where centralized 802.1X authentication is supported. However, means of communicating between authentication server and remote mesh AP is presently not within the scope of the standard.

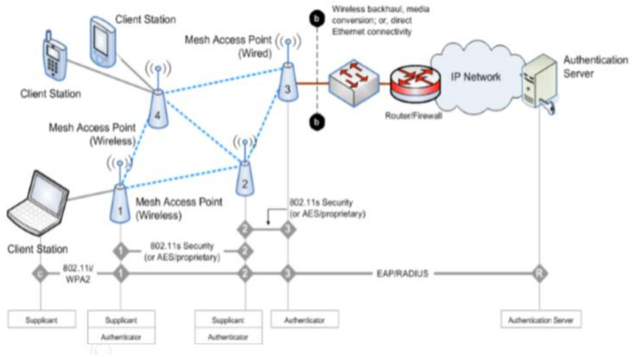


Figure 2: Wireless mesh authentication and encryption

□ The 802.11r standard for client mobility influences the security architecture by enabling a hierarchical key distribution scheme to improve mesh route maintenance. Specifically, this means leveraging key hierarchies and co-ordination with a central/trusted key-holder for pair-wise master keys (e.g., an AP acting as an authenticator will need the pair-wise master keys of the supplicant AP to generate session/transient keys prior to the EAP 4- way handshake).

4. Tools Related with Network Security:

The basic tool related with network security is as follows:

4.1 Network Simulator-1:

The first version of ns, known as ns-1, was developed at Lawrence Berkeley National Laboratory (LBNL) in the 1995-97 timeframe by Steve McCanne, Sally Floyd, Kevin Fall, and other contributors. This was known as the LBNL Network Simulator, and derived from an earlier simulator known as REAL by S. Keshav. The core of the simulator was written in C++, with Tcl-based scripting of simulation scenarios.

4.2 Network Simulator-2:

Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator, the foundation on which NS is invented. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported the development of NS through the Virtual Inter Network Testbed (VINT) project. Currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.

Figure 3 shows the basic architecture of NS2. NS2 provides users with an executable command "ns" which takes one input argument, the name of a TCL simulation scripting file. In most cases, a simulation trace file is created and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles.

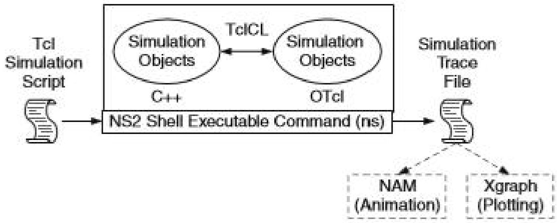


Figure 3: Basic Architecture of NS2

Conceptually, a handle is just a string (e.g., "_o10") in the OTcl domain and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects. It may define its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures (instprocs) and instance variables (instvars), respectively.

4.3 Network Simulator-3:

NS-3 has been developed to provide an open, extensible network simulation platform, for networking research and education. In brief, ns-3 provides models of how packet data networks work and provides a simulation engine for users to conduct simulation experiments. Some of the reasons to use ns-3 include to perform studies that are more difficult or not possible to perform with real systems, to study system behavior in a highly controlled, reproducible environment, and to learn about how networks work. Users will note that the available model set in ns-3 focuses on modeling how Internet protocols and networks work, but ns-3 is not limited to Internet systems; several users are using ns-3 to model non-Internet-based systems.

Many simulation tools exist for network simulation studies. Below are a few distinguishing features of ns-3 in contrast to other tools.

- NS-3 is designed as a set of libraries that can be combined together and also with other external software libraries. While some simulation platforms provide users with a single, integrated graphical user interface environment in which all tasks are carried out, ns-3 is more modular in this regard. Several external animators and data analysis and visualization tools can be used with ns-3. However, users should expect to work at the command line and with C++ and/or Python software development tools.

- NS-3 is primarily used on Linux systems, although support exists for FreeBSD, Cygwin (for Windows), and native Windows Visual Studio support is in the process of being developed.

5. Comparison of Review Techniques:

Network Security Protocols	Performance Parameters	Objective	Tool	Pros	Cons
Simultaneous Authentication of Equals and Efficient Mesh Security Association [1]	Throughput, Average end to end delay	cost-effective communications for deployment in various smart grid domains	NS-3	High throughput for SAE and EMSA (Merkle Tree Authentication)	Less throughput for SAE as compare than EMSA (Black Hole Attack)
EAP-based authentication [2]	Average delay time	Effective security considerations with regard to wireless environments	NS-2	More delay time for EAP-AP	Less delay time for EAP
Mesh Network Security Technology and Threads [3]	Throughput, Delay and Packet Delivery Ratio	Resolve problem of DoS and ToS	Omnet	High Packet Delivery Ratio for AODV protocol	Low Packet Delivery Ratio for DSDV protocol
Wireless Mess Network Protocol [4]	Throughput, Delay Time, Packet Delivery Ratio	low cost, high speed links in wireless networks	NS-2	security measures for SDG against intrusion of a malicious node to provide the availability of effective communication in SG	PDR low for DSDV protocol
Intrusion Detection System (IDS) [5]	Computational Complexity and Communication Overhead	Intrusion Detection and authentication with data fusion in MANET	NS-2	improve the security performance in high-security MANETs.	High delay time
EAP-TLS handshake and the 4-way handshake phases [6]	knowMasterkey, LTShandshake	mutual authentication between supplicant and authentication server in Wireless Network	NS-2	a new effective DoS attack by blocking message 4 has been identified and analyzed	Update value of sn at regular time interval

6. Conclusion:

Traditional wireless networks are moving towards digitally enabled smart grids which will enhance communications, improve efficiency, increase reliability, and reduce the delay time of data packets across the network. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber attacks. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level. In this paper, we surveyed the vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions.

7. References:

[1] Bin Hu and Hamid Gharavi, “Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkle Tree 4-Way

Handshaking", IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 2, MARCH 2014.

[2] JYH-CHENG CHEN AND YU-PING WANG, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", IEEE Radio Communications, December 2005.

[3] A. Gerkis, J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute, 2000 – 2005.

[4] S. K. Saranya, Dr. R. Karthikeyan, "Security for Smart Distribution Grid By Using Wireless Communication" International Journal of Innovative Research in Computer and Communication Engineering, March 2014.

[5] K. K. Lakshmi Narayanan, A. Fidal Castro, "High Security for Manet Using Authentication and Intrusion Detection with Data Fusion", International Journal of Scientific & Engineering Research, March -2012.

[6] Abdullah Alabdulatif, Xiaoqi Ma, "Analysing the EAP-TLS Handshake and the 4-Way Handshake of the 802.11i Standard", International Journal for Information Security Research (IJISR), Volume 3, Issues 3 and 4, September/December 2013.

[7] Luis Carlos Wong, "An Overview of 802.11 Wireless Network Security Standards & Mechanisms", SANS Institute, October 2004.

[8] Zahra Alishahi, Javad Mirabedini and Marjan Kuchaki Rafsanjani, "A new method for improving security in MANETs AODV Protocol", Management Science Letters 2 (Aug. 2012).

AUTHOR'S PROFILE

Sandeep Shivhare has received his Bachelor of Engineering degree in Information Technology from Laxmi Narayan College of Technology, Indore in the year 2010. At present he is pursuing M.Tech with the specialization of Computer Science Engineering in Millennium Institute of Technology, Bhopal. His area of interest is Data Mining, Image Processing etc.

Sriram Yadav has received his M.Tech from Berhampur University, Orrissa. Pursuing Ph. D in CSE from P.A.H.A.R University, Udaipur (Rajasthan). At present he is working as an Associate Professor and Head (PG) in Millennium Institute of Technology, Bhopal. His areas of interests are Data Mining, Image Processing, Cloud Computing, Grid Computing, Video Processing etc..

Madhuvan Dixit has received his M.Tech from RGPV University, Madhya Pradesh. At present he is working as an Associate Professor in Millennium Institute of Technology, Bhopal. His areas of interests are Data Mining, Image Processing, Cloud Computing, Grid Computing, Video Processing etc.