Security of a Mesh Potato Network in Ad Hoc Mode

Hope R. Mauwa and William D. Tucker
Department of Computer Science, University of the Western Cape
Private Bag X17, Bellville 7535, South Africa Tel: +27 21 959 3010, Fax: +27 21 959 1274
email: {**3364810**, btucker}@uwc.ac.za

Abstract – Wireless Mesh Networks can provide low cost and reliable community-owned connectivity in developing rural areas. A rural community can use mesh networks to access a wide range of modern information and communication technologies, and as such, protection of these networks from malicious behavior is very important. While there has been work into securing mesh networks, almost none of it has been applied within the Village Telco, or mesh potato, arena. It is against this background that this paper advocates the investigation of security weaknesses of and solutions for mesh potato networks by intervening with a particular security set-up of the mesh potatoes used in the deployment of a rural community wireless mesh network in Mankosi Community located in the Eastern Cape Province in South Africa. These devices currently have no protection in ad hoc mode. This work in progress paper describes how we plan to provide and test security for this mesh.

Index Terms— Limited Range Communications: Ad-hoc, WiFi; Internet Services & End User Applications: Cryptography.

I. INTRODUCTION

This paper describes work in progress to provide security for a wireless mesh network (WMN) deployed in a rural community called Mankosi, located in the Eastern Cape province of South Africa. The primary objective of this study is to secure the network in ad hoc mode. There has been a lot of research into mesh security. The main problem is that the mesh potatoes (MP), the routers used in the wireless mesh network in Mankosi, provide no security at all in mesh mode. The ethos of the open-hard/software approach to a Village Telco (see www.villagetelco.org), says it is community-owned, ground-up and therefore, anyone ought to be able to get on the network with a mesh potato and make VoIP calls within the mesh for free; hence, no security. However, the Tribal Authority (the informal governance structures) of Mankosi is intent on charging for local in-mesh calls, and to use revenues for network maintenance and expansion. Because we need security, then, there is the technical problem of distributed authentication, which is the suitable security approach for ad hoc mode. This project is an exploration of the balance between these social and technical goals.

There is need to learn how to secure the ad hoc side of the network so that access to and on the network can be controlled. Certificate authority is commonly used for most existing mesh networks, and CA is problematic; central authentication has a single point of failure and cannot work well where members constantly need to renew or revoke their membership in the network like in a mesh network. Therefore, this project involves surveying the existing literature on mesh network security in order to ascertain which mechanisms are most appropriate for a mesh potato network, and how best to implement them on the devices to support ad hoc mode.

II. BACKGROUND

The Bridging Application and Network Gaps (BANG) group in the Department of Computer Science at the University of the Western Cape (UWC), through consultations with the rural community, implemented a wireless mesh network in the rural community of Mankosi in 2012. The network currently has a dozen MPs, with some links up to several kilometres. A mesh potato is a marriage of a low-cost wireless access point capable of running a mesh networking protocol with an Analog Telephony Adapter (ATA) [1]. The MPs multiplex infrastructure and ad-hoc modes, thus providing a widely distributed hotspot.

Three wireless security protocols are available in infrastructure mode: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protection Access Version 2 (WPA2/802.11i). There is not any security mechanism provided for ad-hoc mode. That means packets are exchanged between the mesh stations unencrypted and any MP can join the network if the Service Set Identifier (SSID) is known; a situation that attackers can easily exploit. Consequently, the security of the network in ad hoc mode must be addressed.

III. RELATED WORK

Mesh networks are a type of ad-hoc network and access control in ad-hoc networks is a persistent challenge [2]. Approaches include centralized authentication, distributed authentication and some encryption methods. It is important to note here that there appears to be no recent work that discusses a different approach from the ones mentioned above. This section discusses proposals based on asymmetric cryptography to secure ad hoc networks.

Dahill *et al.* [3] propose a security protocol called Authenticated Routing for Ad hoc Networks (ARAN), in which every node forwarding a route request and route reply message must sign it. Although their approach could provide strong security, placing a digital signature on every routing packet could lead to performance bottleneck on computation in the mesh nodes as they have restricted memory and processing power [4]. Zapata [5] proposes a Secure Ad hoc On-demand Distance Vector (SAODV) routing protocol, an extension of the Ad hoc On-demand Distance Vector (AODV). SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. The mesh nodes could suffer from high processing overhead associated with an asymmetric cryptosystem, and as such the approach is not suitable for the limited capacity MP.

Some researchers have proposed the use of symmetric cryptography for authenticating ad hoc routing protocols, based on the assumption that a security association (a shared key) between the source node and the destination node exist. For example, Papadimitratos and Hass [6] propose a Securing Routing Protocol (SRP), which can be applied to several existing routing protocols. In this approach, Message Authentication Code (MAC) along with shared key is used to provide end-to-end security.

The protocols discussed above except [3] make an assumption that there is a centralized global trusted certificate authority (CA) providing efficient key distribution and management in the network [4]. But central authentication has a single point of failure; when central device is not available there is no way to renew or revoke other members [2]. To mitigate this problem, the concept of threshold secret sharing has recently been introduced [4]. Zhou and Haas [7] use a partially distributed certificate authority scheme in which a group of special nodes is capable of generating partial certificates using their shares of the certificate-signing key. A valid certificate can be obtained by combining a certain fixed number of such partial certificates. The weakness of the solution is that it requires an administrative infrastructure available to distribute the shares to the special nodes. Deng *et al.* propose another approach based on threshold secret sharing; but instead of using the traditional public key cryptography mechanism, they use an identity-based cryptosystem to provide end-to-end authentication [4]. In this approach, the capabilities of certificate authority (CA) are distributed to all the nodes in the network and any operations requiring the CA's private key can only be performed by a coalition of certain number of nodes. Distributing the CA to all the nodes in the network provides good availability since all nodes are part of the CA service.

IV. METHODOLOGY

This work intends to provide the security for a rural WMN in mesh mode on the mesh potato platform. To achieve that, our research entails the following research questions: which security mechanisms are necessary and appropriate in WiFi mesh mode? How can we implement them in mesh mode on the mesh potato? Which mechanisms are secure for the mesh mode of mesh potatoes? A security mechanism, which is secure and applicable to mesh potatoes in Wi-Fi mesh mode, will be determined. Only mechanisms that include encryption of the payload as one of the security components will be considered. To do this, we will follow an experimental research methodology with practical trials and experiments conducted in a research laboratory followed by in-the-field trials on the rural WMN. A qualitative evaluation with mesh end users will complement the pursuit of technical security validation.

V. CONCLUSION AND FUTURE WORK

The security weaknesses of the mesh nodes potatoes in the mesh network implemented in Mankosi have been identified. The next step is to do a critical analysis of existing security mechanisms for mesh networks, which has commenced via a literature review to identify mechanisms that are applicable in ad hoc mode. Once identified, we will inject security functionality into the MP firmware and carry out experimentation in the laboratory. To identify which mechanism or combination of mechanisms is truly secure for the mesh potatoes, we will identify, explore and adapt WiFi cracking software tools, which are freely available from the Internet. Then we will evaluate the mechanisms in the laboratory by conducting trials with these software tools. The ones that are resistant to the cracking software will be considered for incorporation into the mesh potato platform, and tested on the Mankosi rural mesh network.

In conclusion, the security of wireless mesh networks is an ongoing research challenge, and in particular, has not yet been provided for in the mesh potato domain. This project seeks to rectify that problem and as an outcome provide a framework and guidelines for the injection and verification of security mechanisms into ad hoc mesh platforms, using the mesh potato platform as an experimental example.

VI. ACKNOWLEDGEMENTS

We thank Telkom, Cisco, Aria Technologies and THRIP (Technology and Human Resources for Industry Partnership) for their financial support via the Telkom Center of Excellence (CoE). This work is based on the research supported in part by the National Research Foundation of South Africa (Grant specific unique reference number (UID) 75191). Any opinion findings and conclusion or recommendations expressed in this material are those of the authors and therefore the NFR does not accept any liability in this regard.

VII. REFERENCES

[1] Adeyeye M & Gardner-Stephen P (2011). The Village Telco project: a reliable and practical wireless mesh telephony infrastructure. *URASIP Journal on Wireless Communications and Networking.* 1-11.

[2] Saay MS (2011). *Toward Authentication Mechanisms for Wi-Fi Mesh Networks, Unpublished MSc thesis.* Computer Science, University of the Western Cape, Cape, South Africa.

[3] Dahill B, Sanzgiri K, BN Levine, Shields C & EM Belding-Royer (2002). Authenticated Routing for Ad hoc Networks. *IEEE International Conference on Network Protocols (ICNP).*

[4] Deng H, Mukherjee A & Agrawal DP (2004). Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks. *IEEE International Conference on Coding and Computing*. 107 - 111.

[5] Zapata, MG (2002). Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106-107.

[6] Papadimitratos P & Haas ZJ (2002). Secure Routing for Mobile Ad Hoc Networks. *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference.*

[7] Zhou L & Haas ZJ (1999). *Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security*. 11.

Hope Mauwa received his BSc in 2002 and MSc degree in Information Technology in 2007 from University of Malawi and Nelson Mandela Metropolitan University, respectively. He is presently pursuing a PhD in Computer Science at UWC, and is also a member of BANG research group. His research interests include mesh network security, information security and ICT4D.