

# Self-Organizing Security Scheme for Multi-hop Wireless Access Networks<sup>1,2</sup>

Lusheng Ji, Brian Feldman, Jonathan Agre  
Fujitsu Laboratories of America  
8400 Baltimore Ave., Suite 302,  
College Park, Maryland 20740, U. S. A  
301-486-0398  
{lji, bfeldman, jagre}@fla.fujitsu.com

*Abstract*— A multi-hop wireless access network can provide a rapidly deployable, mobile communications infrastructure that is suitable for many sensor network scenarios. In particular, such a network based on the IEEE 802.11 wireless local area network (WLAN) protocols can be economically built allowing sensors equipped with standard network interface components to communicate. However, improved security for these extended multi-hop WLANs is required. In this paper, the WPA protocol for security on an IEEE 802.11 WLAN is extended to operate on an ad hoc wireless multi-hop network. A method is described for applying the WPA protocol beyond the single-link case for which it was defined, to a store-and-forward wireless network. In particular, the Secure Nomadic Wireless Network (SNOWNET) system is described that implements a collection of access networks interconnected via a wireless ad hoc backbone network. Each SNOWNET node is a router that has both an access service and a wireless backbone interface. The backbone is automatically formed as an ad hoc network among the routers using MANET-style routing schemes for data forwarding. The security method described will provide data protection and authentication for client users, attached sensor devices and for the routers that may dynamically join and exit from the backbone network.

## TABLE OF CONTENTS

<b>1. INTRODUCTION</b> .....	1
<b>2. BACKGROUND</b> .....	2
<b>3. SNOWNET OVERVIEW</b> .....	4
<b>4. SNOWNET SECURITY</b> .....	5
<b>5. CONCLUSION</b> .....	9
<b>REFERENCES</b> .....	9

## 1. INTRODUCTION

The use of IEEE 802.11 wireless local area network (WLAN) technologies has become commonplace, the costs

of the equipment have fallen drastically, the size of the network interface cards has been reduced (e.g., Smart Disk form factor is now commercially available) and the software has become robust and available on many different platforms. In effect, it is now a commodity with the attendant advantages of economies of scale and rapid technological improvement. The data rates of IEEE 802.11 radios have quickly evolved from 1 megabits per second (mbps) to over 100 mbps (e.g., in commercial variants of IEEE 802.11a/g). As a result, providing a networking infrastructure from 802.11 technology for low-cost sensors is now feasible from a cost and performance perspective. Several key aspects of such an infrastructure include rapid deployment, portability, self-configuration, wireless multi-hop data forwarding and security.

One such system, the Secure Nomadic Wireless Network (SNOWNET), was designed as a wireless access network technology that is portable, rapidly deployable, and secure [1]. It combines a wireless multi-hop backbone network with infrastructure-mode IEEE 802.11 network access services. SNOWNET router nodes have multiple WLAN radios and are used as both standard WLAN Access Points (APs) and backbone routers. The advantage of using SNOWNET is that in order to extend WLAN coverage to a new area that does not have an existing infrastructure network, we only need to deploy new SNOWNET nodes in the new coverage area. They will automatically form a wireless multi-hop data forwarding network connecting the new area to the rest of the SNOWNET. At the same time these new SNOWNET nodes provide AP access service to their coverage areas. Sensor devices are equipped with standard IEEE 802.11 client network interface cards, as well as users, attach to the nearest SNOWNET router providing access service. SNOWNET is an all-IP network and will forward the sensor data within the network or to gateway routers. SNOWNETs are being applied to many applications including sensor and surveillance networks, emergency responder communications, embedded WLAN networks and hotspots extensions where cabling is not feasible.

<sup>1</sup> 0-7803-8155-6/04/\$17.00© 2004 IEEE

<sup>2</sup> IEEEAC paper #578, Version 2, Updated November 13, 2003

Security is one of the key requirements in these applications and it is a major element in the design of SNOWNET. The difficulties involved in providing security in traditional IEEE 802.11-based systems are now well known. In fact, one of the major recent events within the security research community was the discovery of the flaws in the IEEE 802.11 WLAN specification's Wired Equivalent Privacy (WEP) mechanism [2]. Unfortunately, by the time the weaknesses of WEP were published [3,4,5,6], the IEEE 802.11 technology had already been so successful in the market that it was too late to make any major changes to the standard.

It became obvious at that time that a new security mechanism must be developed to replace WEP. Other than the usual technical issues involved in the design of a new security system, the security research community was faced with another problem: given the fact that so many WEP-based 802.11 devices had been manufactured and sold, what kind of new security mechanism could be introduced that would strengthen security while still preserving user and infrastructure investments in existing IEEE 802.11 hardware and software. The solution proposed by the WiFi Alliance was called the Wi-Fi Protected Access (WPA) scheme [7].

WPA attempts to address all the known attacks to the WEP. It uses a different authentication architecture from the WEP and has a fundamentally different way of using the encryption keys, but it still uses the same basic building blocks for its data privacy and integrity protection as WEP. Thus, most of the existing IEEE 802.11 network interface cards are able to support WPA through upgrading only the driver software and embedded firmware.

However, the design of WPA focused on infrastructure mode IEEE 802.11 WLANs, which is the mode under which the majority of WLANs operate. In an infrastructure mode WLAN, there are two types of devices, Access Points (APs) and clients. The clients acquire network access services through connection to an AP. The APs may be interconnected by another network named the Distribution System (DS), but this interconnection is not required. WPA security protects the wireless links between the APs and clients. The DS is assumed to be a trusted network and needs to exist before any WLAN APs are installed. This requirement greatly limits flexibility, as the APs can only be deployed at locations where the trusted network infrastructure already exists. There are no dynamic and automatic mechanisms that will extend the trusted network infrastructure to where a WLAN is needed.

In this paper, we focus on the approach taken to provide a high level of security in SNOWNET for clients, devices such as sensors, and for the multi-hop backbone network. The guiding principles for this network are to 1) support standard WLAN network interface devices as clients

without requiring modifications and 2) self-organization of the backbone network for ease of deployment and portability. Following these principles, we have developed extensions to the typical link-based security mechanisms that are required to operate in a multi-hop environment.

## 2. BACKGROUND

In this section, we present a summary of many of the WLAN security issues. A description of WEP and its improvements, such as the new IEEE 802.11i and especially WPA, is provided prior to describing the design choices and details of the SNOWNET security mechanisms.

### 2.1 Wireless Equivalence Privacy (WEP)

WEP claims to offer three types of security to a reasonable degree: data privacy, data integrity, and client authentication. Data privacy is guarded by encryption. WEP uses a symmetric, shared key between two communicating devices, i.e. a client and an AP. This shared WEP key is then used by the RC4<sup>3</sup> algorithm to generate a pseudorandom stream of bits called the key stream. The bits from the key stream are then XOR-ed with plaintext data bits to produce the ciphertext. Every time that a data packet needs to be encrypted, the key stream generated by the RC4 should be different. To achieve this, WEP uses an Initial Vector (IV), a 24-bit number that is changed for every data frame, together with the shared WEP key as the two inputs into the RC4 algorithm. Only the IV is included in each data frame so that the receiver can generate the same RC4 key stream as the sender for decoding, using the enclosed IV and the shared WEP key. WEP specifies a shared secret 40 or 104-bit key to encrypt and decrypt the data.

For protecting data integrity, WEP uses an Integrity Check Value (ICV), which is a 32-bit Cyclic Redundancy Check (CRC) value, for each data packet to be sent. This ICV is then appended to the data frame and the resulting message is then encrypted by WEP.

The shared-key type of authentication process consists of the client and the AP exchanging WEP encrypted challenge/response texts. The logic behind the WEP-based authentication is that if the response text matches with the challenge text, the client must know the same shared WEP key as the AP, hence the client is authenticated.

Thus the shared WEP key plays a critical role in all WEP security procedures and it must be well guarded. Unfortunately, WEP does not specify an adequate shared WEP key management and distribution mechanism. In most deployments the shared keys are configured manually, making it difficult to change the key in a deployed system as all user devices need to be updated.

---

<sup>3</sup> RC4 is an efficient stream cipher with a long period commonly used in encryption, designed by R. Rivest, RSA Security, Inc.

Various papers describing different attacks [3,4,5,6] conclude that 24 bits for the IV is not enough. After sending out only  $2^{24}$  packets, IVs have to be reused (called IV collision). An attacker can easily identify what packets are encrypted by the same key stream resulting from a reused IV (since IVs are included in the data frames as plaintext). After identifying and collecting enough of such data frames, the attacker can break the shared WEP key from these data frames. In [6] the authors identified another problem of RC4 in that some keys are recognized as “weak keys”. If a weak key is input to the RC4 algorithm, the initial portion of the pseudo-random stream becomes highly predictable and the chance of the shared key being broken is greatly increased. Due to the central role of the shared key in the WEP protection properties, if the key is broken, all WEP protections are gone.

## 2.2 Improvements to WEP

### 2.2.1 IEEE 802.1x

After the weakness of WEP was revealed, WLAN equipment vendors have been introducing various improvements. Limited by the need to be backward compatible and given the capability of existing IEEE 802.11 chipsets which are designed and manufactured to only support WEP, these improvements focus mostly on WEP key management while still using WEP to protect data privacy and data integrity.

The major problem of WEP is the lack of a convenient and automatic WEP shared key update method, resulting in the shared key reuse flaw. One approach is to ensure that the shared WEP key is updated quickly and frequently enough so that before an attacker has enough time to break the current shared WEP key, the key is already changed. In order to accomplish this property, vendors proposed combining two security protocols: the Extensible Authentication Protocol (EAP) [8] (initially developed for the Internet) and an IEEE 802.1x [9] based authentication framework for both client and access point mutual authentication and session key delivery.

The IEEE 802.1x is a port-based, access control framework for wired or wireless networks that decides whether a client is authorized to use the network access service and then implements the decision. There are three types of entities in the IEEE 802.1x framework: supplicants, authenticators, and an authentication server. A supplicant is a client who wishes to use the network access service. An authenticator is a device which separates the supplicant from the rest of the network, i.e. an AP, and prevents unauthorized access. The authentication server is a backend server which makes the decision of granting or denying the supplicant’s request. After the decision, the authenticator either blocks the supplicant’s data traffic or lets it pass through.

IEEE 802.1x messages are transmitted using two versions of the EAP over two types of connections: 1) the link layer

(LAN or WLAN) connections between the authenticators and supplicants and 2) the transport layer connections between the authenticators and the authentication server. For the first type of connection, IEEE 802.1x defines the Extensible Authentication Protocol over LAN (EAPOL). For the second type of connections, although the IEEE 802.1x does not define its own protocol, installations have been using a protocol based on the specifications defined by the “EAP over RADIUS” standard [10] (the Remote Access Dial-In User Services itself is defined in [11]).

A typical IEEE 802.1x authentication session starts when the client (supplicant) sends an EAPOL-Start message to an access point (authenticator) indicating its interest in using network access service. Upon receiving this message, the authenticator sends back an EAP-Request/Identity message. The supplicant must respond with an EAP-Response/Identity message. After receiving the supplicant’s identity, the authenticator then needs to contact the authentication server by forwarding the supplicant’s identity response to it. From this point on, the authentication message exchanges are between the supplicant and the authentication server. The details of the message exchanges depend on the actual authentication (referred to as Upper Layer Authentication or ULA) algorithm being used. The IEEE 802.1x supports a number of such ULA mechanisms such as the Transport Layer Security (TLS) [12] and the Kerberos V5 [13]. Although all ULA messages pass through the authenticator, the authenticator needs not understand any of them. At the end of the authentication sequence, the authentication server makes a decision of either granting or denying the supplicant’s access request. The decision is sent to the supplicant in an EAP-Success or EAP-Failure message. When the authenticator is forwarding this final Success/Failure message to the supplicant, it too understands the message and hence executes the decision to either allow or block the supplicant’s data traffic.

The IEEE 802.1x authentication described above only deals with the initial authentication of the client and is susceptible to certain attacks such as session hijacking. It does not really bind the supplicant and authenticator together. The most common solution to secure-binding between two entities is to establish a session key only between these two entities, for example as described in a Microsoft extension to RADIUS [14]. At the end of RADIUS authentication, the RADIUS server generates a session key for the supplicant. This session key is sent to the supplicant securely as part of the authentication procedure. The same session key is then sent to the authenticator using the Microsoft extension. This session key is used for encrypting data between this particular pair of supplicant and authenticator, hence preventing potential session hijacking.

### 2.2.2 Wi-Fi Protected Access (WPA)

Additional improvements are being considered by the IEEE 802.11i working group on security based on a new security approach for WLANs expected to be a complete replacement of the WEP [15]. The IEEE 802.11i standard is being developed with significant security research community involvement and it reflects the experiences and lessons learned from WEP, providing protection against all known attacks to WEP. It is considered to be the next generation security standard for IEEE standards-based WLANs. Currently the IEEE 802.11i standard is in draft stage and is expected to be standardized near the end of 2004.

Meanwhile, before new hardware that fully supports the IEEE 802.11i are manufactured and shipped, the Wi-Fi Alliance<sup>3</sup> of the IEEE 802.11 product manufactures is pushing a compromise solution which balances both the achievements of the IEEE 802.11 task group and the reality of the large number of existing WEP-only IEEE 802.11 devices. Their effort focuses on a subset of the IEEE 802.11i standard that is compatible with most of current WEP-capable hardware, called the Wi-Fi Protected Access (WPA) [7]. WPA also follows the IEEE 802.1x architecture, and requires the authentication procedure described in the previous section. In addition, WPA includes a new way of using encrypting data through the Temporal Key Integrity Protocol (TKIP). For most of the existing WEP-capable IEEE 802.11 devices (including both client devices and access point devices), TKIP can be supported with only a firmware and software upgrade.

WPA has a more secure method of using the keys. Instead of using a single shared key for everything, WPA uses four 128-bit keys for protecting each pairwise communication: one pair of keys for protecting data encryption and data integrity and one pair of keys for protecting the communication between the two devices during their initial handshake. Collectively these four keys together are known as the Pairwise Transient Keys (PTK). Similarly each one-to-many group communication session is also protected by a Group Transient Key (GTK). The transient keys are changed for every data packet sent.

Despite the fact that so many keys are used, WPA only requires the configuration of one single key, the master key, for each pair of communicating devices or each group communication source. All other keys are derived from the master keys. Such a key organization is called a key hierarchy. In WPA, the pairwise master keys are a by-product of the authentication process as they are the session keys established by the RADIUS server at the end of the authentication procedure. Group master keys are separately selected by the group communication sources.

The PTKs are never exchanged between a pair of communicating nodes. Instead, they are computed

independently by these two nodes. A four-way handshake is designed as part of TKIP to exchange the PTK computing parameters between a pair of nodes. The key generating parameters include such values that with extremely high confidence, the resulting transient key will be different for every time and every pair of nodes. At the end of this four-way handshake, both sides will have the same key generating parameters so they can generate the same PTK. Also proven during the handshake is that both sides know the same master key and therefore mutual authentication is achieved. After the PTKs are computed, GTKs are computed only by group communication sources and delivered to receivers via the already secured pairwise communications between the sources and receivers. GTKs may need to be re-computed and re-distributed from time to time due to group changes.

The data encryption keys of the PTKs and GTKs are then used by TKIP to generate a per-packet key, which is sent to the RC4 algorithm along with an IV to generate the key stream. Unlike in WEP where the shared key is used directly by RC4, TKIP performs per-packet key mixing and only the result is used by RC4. Hence the data encryption key of TKIP is much better protected. In addition the TKIP IVs are 48 bits long. With such a huge IV space, IV collision is not expected to occur and known weak keys can also be avoided. The IVs are also used by TKIP as data frame sequence numbers to prevent replay attacks.

## 3. SNOWNET OVERVIEW

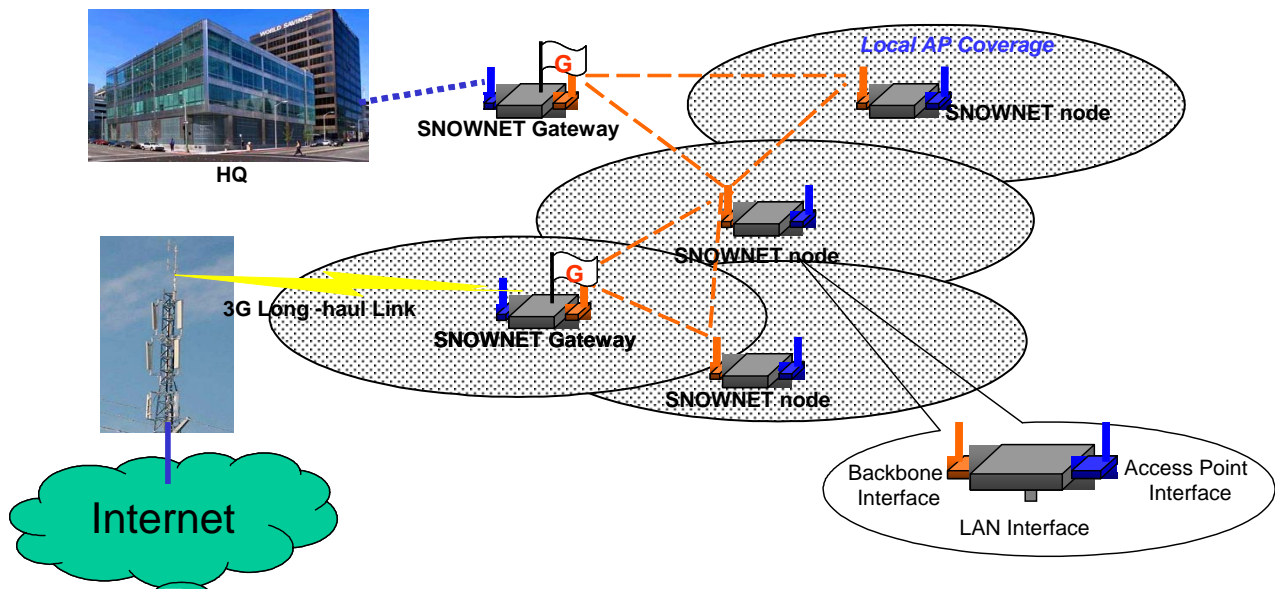
The Secure Nomadic Wireless Networks (SNOWNET) is a new type of multi-hop wireless access network currently under development [7] that combines Mobile Ad hoc Network (MANET) technologies [16] with WLAN access services. SNOWNET forms a two-layer hierarchical network as shown in Figure 1.

In the bottom layer, SNOWNET nodes provide standard WLAN access services to sensors and other regular clients with standard IEEE 802.11 interface cards. Hence, normal clients may connect to SNOWNET in the same fashion as they connect to any other standard WLAN. In the top layer, SNOWNET nodes form a wireless backbone network among themselves. Thus the deployment topology of the wireless network is no longer constrained by the fixed connections to a wired network infrastructure, permitting changes in SNOWNET node locations. Links between nodes are dynamically established subject to the communication parameters and range constraints of the physical environment. Through topology information exchange, the SNOWNET data forwarding protocol is able to dynamically adjust and self-organize the data forwarding routes based on the current topology of the wireless backbone and the current attachment distribution of clients. Thus, SNOWNET nodes are portable and the configuration of the network can adapt to changing usage patterns by adding, deleting or moving of nodes.

The original data forwarding protocol supported was designed for storing-and-forwarding of IP traffic only [1]. However, in order to implement the security mechanism, an extension to this protocol was required that includes the link layer identities (e.g., MAC addresses) of the SNOwNET nodes in the topology information exchange and route computation. This enables the extended forwarding protocol to compute routes for data link layer frames even if the destination is several hops away. A new encapsulation mechanism, called SNOwNET envelopes, was hence developed for forwarding data link layer frames across an arbitrary network layer topology. Schemes such as ARP, reverse ARP and Proxy ARP typically assume a more restrictive network topology and broadcast domain configuration.

local access service in their service coverage area. When SNOwNET is not deployed as a standalone network, some nodes will need to have connectivity to an external organizational network or the Internet. These nodes provide the gateway service and thus become the “gateway nodes” for the other SNOwNET nodes to route traffic to reach the external network or Internet. In the following context, we may refer to a particular service interface as “node” since it is more conventional and intuitive to use the term “node” than “interface” when describing network concepts. For instance, we may use the term “backbone node” to refer to the “backbone interface” of a SNOwNET node, which may at the same time using another interface to provide network access service.

Data forwarding in a SNOwNET is similarly organized into



**Figure 1:** Sample SNOwNET Architecture

There are three major functions provided by the nodes: backbone service, access service and gateway service. Every SNOwNET node is equipped with at least one wireless networking interface providing the backbone communications between peer SNOwNET nodes. Optional external antennas may be used to extend the communication range of the backbone interfaces. For maximum flexibility the backbone interfaces of the SNOwNET operate under ad hoc (Independent Basic Service Set, or IBSS) mode. In addition to backbone interface(s), a SNOwNET node may be equipped with additional interfaces to provide local WLAN AP access service to clients. Similarly, it is also possible for a SNOwNET node to be equipped with a wired LAN interface to provide wired LAN access service to clients. In Figure 1, several typical SNOwNET nodes are shown which have two wireless interfaces, one for backbone communications, and the other for providing the

two levels: backbone communication and local access communication. SNOwNET nodes relay communication between these two levels. Therefore a typical intra-SNOwNET communication path includes the link between the source mobile client and the SNOwNET node serving the source client, a number of SNOwNET backbone links, and finally the link between the destination client and its access service SNOwNET node.

#### 4. SNOwNET SECURITY

Corresponding to data forwarding, SNOwNET security is also organized and managed in two levels. Figure 2 illustrates the typical components involved in SNOwNET authentication operations. Differing from typical MANET security approaches [17, 18], SNOwNET focuses on extending the standard IEEE 802.11 security mechanisms,

which are designed for single hop wireless networks, to multi-hop networks. SNOWNET data security is based on WPA security, with modifications accommodating the special characteristics of SNOWNET.

#### 4.1 Client Authentication and Security

On the bottom level, standard WPA security for clients is supported. SNOWNET always assumes that a WPA RADIUS server is either running within the SNOWNET or is reachable from the SNOWNET through a gateway service. Each SNOWNET node that provides AP service supports the functions of an IEEE 802.1x authenticator. When a client is requesting network access service, it begins with an EAPOL-Start message; then, the standard WPA authentication procedure continues as described in Section 2.2.1. After the IEEE 802.1x authentication execution completes, both the client and the SNOWNET node providing AP service will receive a session key from the RADIUS server. The session key is used as the master key for WPA transient key generation. The current group transient key is also generated and sent to the client by the SNOWNET AP node. When a client disassociates from a SNOWNET AP node, the AP node needs to update the group transient key. The new group key is then sent to each attached client of the AP node using EAP-Key messages. In addition to WPA security, SNOWNET also supports

directly. The SNOWNET AP node will automatically regenerate and install new session keys periodically.

#### 4.2 Backbone Authentication and Security

What is more interesting is the security in the backbone network of SNOWNET. The WPA specification does not handle ad hoc links. Only its superset standard, IEEE 802.11i, contains any specifications for providing security to ad hoc links, and in this each ad hoc link is managed individually. The IEEE 802.1x type of authentication is not used, as ad hoc links are thought to be typically created in an infrastructureless network where there would rarely be a RADIUS server available. Two devices interested in communicating via an ad hoc link must have a “pre-shared” key. This key, typically configured manually, is used as the master key in the subsequent WPA transient key generation. The device with lower MAC address will act as the supplicant and initiate the 4-way WPA key material exchange handshake. After the handshake is completed, each end sends its own group key to the other end.

There are two potential problems that preclude us from applying the above proposed IEEE 802.11i ad hoc security mechanism to the SNOWNET backbone, despite the fact that SNOWNET backbone links are indeed ad hoc links. The first problem is the per-shared key requirement. Such a

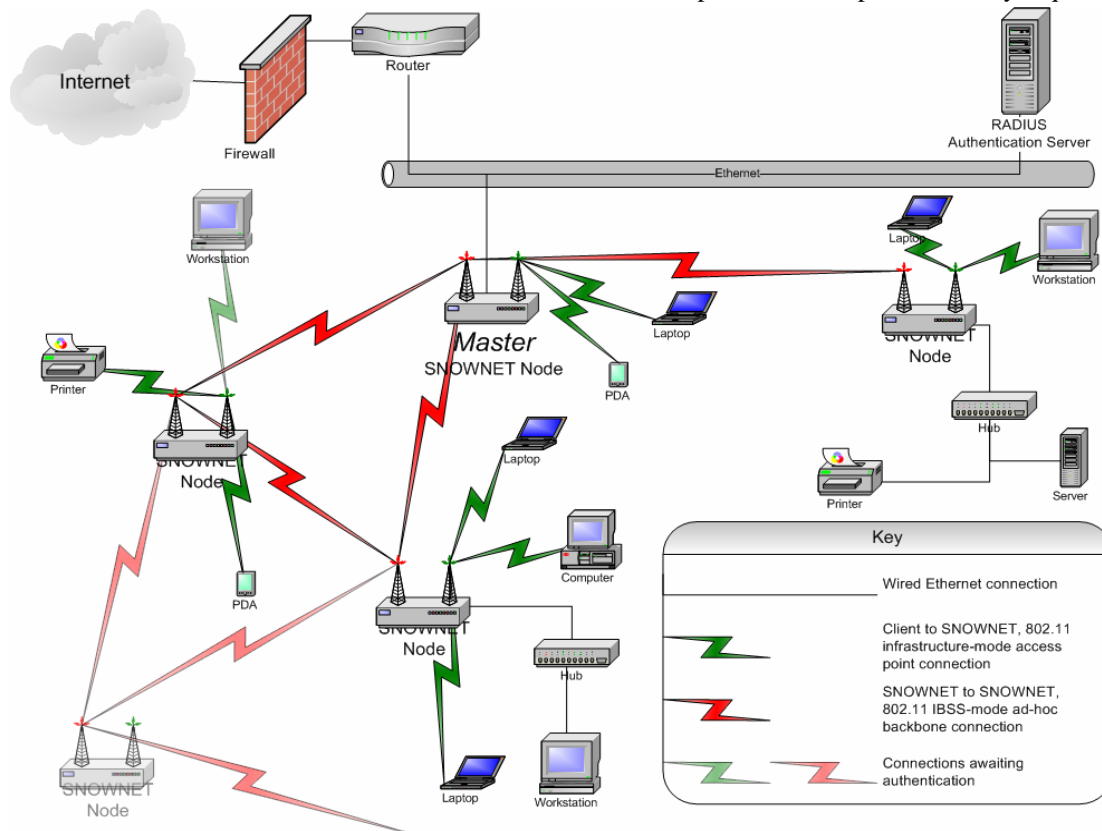


Figure 2: SNOWNET Authentication Architecture

older style security for clients that do not support WPA. In this case the session key is used as the shared WEP key

solution may be acceptable for small networks created in an ad hoc fashion and only existing for a short period of time.

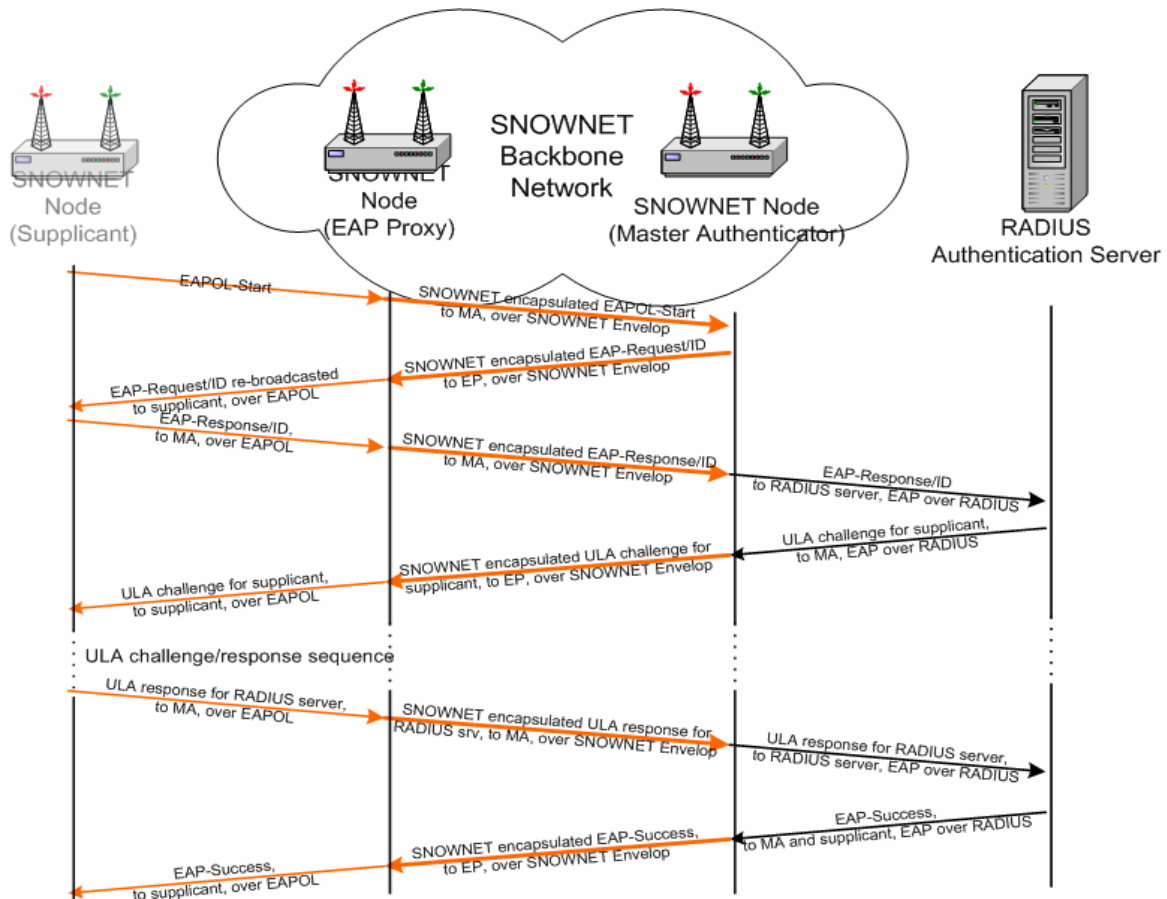


Figure 3 Backbone Authentication Messaging Sequence

But, it does not scale well and it repeats the exact problem of WEP key management if the link is used for an extended period. In addition, in a dynamic ad hoc network where nodes may leave, this approach lacks an efficient mechanism to update the pre-shared key after a node's departure. A SNOWNET backbone network may exist for an extended period of time and the membership and topology of the backbone are dynamic. Therefore, the approach for ad hoc network security of the IEEE 802.11i is not well suited in SNOWNET environment.

The second problem concerns the number of keys used in the IEEE 802.11i approach where each ad hoc link is secured individually. A different WPA transient key (a set of 4 keys) is needed for pairwise communications over each link. Hence there may be up to  $N * (N - 1) / 2$  separate transient keys for pairwise communication within a network of  $N$  nodes. Additional  $N$  group transient keys are also needed. The number of keys managed by the network grows along  $O(N^2)$  and this also does not scale well. To make things worse, most standard IEEE 802.11 hardware designs only allow up to 4 different keys installed in the memory. Any additional active keys can only be installed in the operating system instead of the device, which may result in significant performance drawbacks. In the rest of this section, we describe a new approach for SNOWNET backbone security and node authentication that

differs from the proposed IEEE 802.11i solution for ad hoc links. In our approach, we attempt to extend the WPA's pairwise security model to cover the whole backbone network.

Again, in our approach, we assume that there exists a RADIUS server that is reachable from the SNOWNET. This server may or may not be the same RADIUS server handling client device authentications. Within the SNOWNET backbone, one node acts as the authenticator for the entire backbone network. This node is named the "Master Authenticator (MA)". The identity of the MA is included in SNOWNET topology exchange messages and sent to all authenticated backbone nodes already on the backbone. As a requirement, the identity of the RADIUS server is known to the MA. During SNOWNET deployment, the MA must be the first to be deployed and it must be able to reach the backbone RADIUS server. New backbone nodes are added to the SNOWNET backbone in an iterative manner as they are authenticated by the MA and RADIUS server.

Given this framework, one of the difficulties is how to forward the 802.1x's EAPOL messages. Since all EAPOL messages are link layer data frames, they can not be transmitted between nodes separated by other store-and-forward nodes operating at the network layer. As we have

described earlier, the SNOWNET backbone network is capable of forwarding network layer data packets. Thus, the solution is to encapsulate EAPOL frames in special IP or higher layer packets. A special SNOWNET packet format is defined for encapsulating EAPOL packets, called Envelopes. SNOWNET Envelopes are transmitted across the backbone network just like other user data messages encoded with the encryption mechanism of the SNOWNET backbone.

The SNOWNET Envelope packets are network-or-above layer packets. A TCP packet is the preferred method, although IP or UDP packet may also be used depending on each individual system's requirement and implementation details. However, in the case when an IP packet or UDP packet is used as SNOWNET Envelopes, additional mechanisms are needed to increase delivery reliability. When an EAPOL packet is delivered over a single WLAN link, the sender is able to find out if the receiver has received the packet via a link layer acknowledgement. A similar function needs to be provided for the SNOWNET Envelope packets.

#### *4.3 Backbone Message Exchange*

The messages being exchanged during the authentication stage are illustrated in Figure 3. When a new SNOWNET node tries to join the backbone network, it acts as a supplicant and sends out an EAPOL-Start message. Any SNOWNET backbone node that is within range may receive the EAPOL-Start message. The backbone node hence becomes an EAP Proxy (EP) for the new node and encapsulates the message within a SNOWNET Envelope message addressed to the MA. Multiple SNOWNET nodes may actually receive and forward the EAPOL-Start message as an EP. After being forwarded by the SNOWNET backbone, the Envelope message reaches the MA and the outer Envelope specific fields are peeled off and the EAPOL-Start message is revealed and passed to the authenticator function of the MA. The authenticator selects one of the EP's as the preferred EP and then replies with a standard IEEE 802.1x EAP-Request/ID message. Again, this EAP message is encapsulated in another SNOWNET Envelope message and the Envelope is addressed to the preferred EP. From this point on, the standard IEEE 802.1x style authentication is carried out among the supplicant, the MA, and the backend RADIUS server. For EAP messages from the supplicant to MA (or RADIUS server), the EP receives the link layer frames from the supplicant, encapsulates them in SNOWNET Envelopes and sends them towards the MA. For EAP messages of the opposite direction, the MA will encapsulate those using SNOWNET Envelopes addressed to the EP. The EP then unencapsulates the EAP frames from the Envelopes and forwards the resulting EAP frames to the supplicant over the ad hoc link between them.

Due to the ad hoc and dynamic nature of the network, the

new supplicant will not know a priori the identity of an EP. This is different from authentication between a client and an AP, where the identity of the AP is known to the client. Thus the EAPOL-Start message is sent in plaintext using a link layer broadcast address. Any SNOWNET backbone node who receives and reacts to the message becomes an EP and there may be multiple EPs that forward the EAP-Start message to the MA. The MA selects a preferred EP according to various criteria, such as least loaded node or first arrival, and only uses this EP to correspond with in subsequent steps. EAP messages in subsequent steps from the MA to the supplicant are explicitly addressed to the preferred EP and similarly on the return path. The remaining EPs will drop out of the communications unless a new EAPOL-Start is received.

#### *4.4 Backbone Key Handling*

As a result of the IEEE 802.1x authentication procedure, a session key is established between the new SNOWNET backbone node and the MA and the WPA pairwise transient key is generated from that. After the WPA pairwise key is established, the MA needs to forward the current group key to the new node. The group key is used to protect the communications among all backbone nodes.

It is also the MA's responsibility to generate and update the group key. When a current SNOWNET backbone node leaves the backbone network, it is necessary for the MA to renew the group key. In addition, since not all node departures are known to the MA, the MA will generate this new key on a periodic basis. The choice of a good lifetime of each group key is dependent on the dynamics of the network and is the subject of more study. A new group key is delivered from the MA to all SNOWNET backbone nodes individually via EAP-Key messages protected with the pairwise EAP-Key encryption keys and integrity keys derived from the authentication procedure.

Newly generated and distributed group keys are not effective immediately but are scheduled to be used at a future time. The gap between the current time and the new key effective time should be long enough to assure that the new group key is received by all backbone nodes with high likelihood and to allow for any backbone node to specifically request the new key if it is believed to have missed the delivery of the new key (e.g. because of lost packets). Although the new group key is not used immediately, it is installed into the IEEE 802.11 hardware as a secondary key. After the new group key goes into effect, the old group key is also kept in the hardware as a secondary key for a short period of time. There is a time window during which both new and old group keys are accepted for decryption to accomplish the key synchronization among all backbone nodes. Depending on the settings of various timer values, more than one group key may be transmitted to the new node. Among these keys,

one is used as the current effective communication key and the rest will be used as future communication keys.

The MA is critical in SNOWNET backbone security as the pairwise security binding is only between the MA and other SNOWNET backbone nodes. The total number of WPA transient keys the MA needs to maintain for a backbone network of  $N$  nodes is  $N$ , with  $N - 1$  TKIP pairwise transient keys and 1 group key. The number of keys being managed by the network grows as  $O(N)$ .

SNOWNET backbone communications are encrypted with the group transient keys. This transient group key is used as the temporal key in the TKIP phase 1 key mixing. If TKIP is not supported in a particular implementation of SNOWNET node hardware and firmware, the group key may also be directly used as a WEP key (a hash function is needed to format the transient group key into a key format compatible to WEP). However, in this case most of the problems associated with WEP would remain unsolved. The advantage of using SNOWNET security mechanism in this case is that the MA is able to generate and deliver new group keys to all backbone nodes across a multi-hop network so that each group key only has a short lifetime and during which attackers are unlikely to gather enough packets to break the key.

## 5. CONCLUSION

In this paper, we have introduced our approach to extending the new WLAN security mechanism, WPA, to provide security in dynamic multi-hop wireless access networks for sensor networks and other applications. Current specifications of WPA only support WLAN operation in infrastructure mode over a single link. However, it is also desirable to provide strong security to ad hoc or IBSS links used in multi-hop networks. Using our SNOWNET architecture, as an example network, we describe the particular methods in which we extended and incorporated the WPA's security framework.

With respect to security, some immediate remaining problems to be addressed in the near term include determining an optimal timeout period for the keys, reducing the encryption overhead and examining the performance in large deployments. Since networks such as SNOWNET may be deployed in battlefield or disaster relief operations, very robust security is required. To this end, we would like to further distribute the functions of the Master Authenticator to the end-nodes themselves and to have more efficient mechanisms for recovering from MA failures. Also, mechanisms to prevent the physical compromise of sensitive information stored within the SNOWNET nodes have been considered. We are also looking into providing some security policy enforcement mechanisms in the SNOWNET nodes themselves.

Other more generic issues that will be addressed relate to

trust mechanisms on the backbone. In the current solution, potential supplicants, be they user clients, sensor devices or backbone routers, need to have some a priori information, such as a certificate, that can be verified by the IEEE 802.1x authentication servers. In the future, the nodes may be equipped with other forms of authenticating information such as biometrics or special purpose key generators to increase the ability to form spontaneous networks. Further, mechanisms based on observing behavior over a period of time may also be incorporated for building trust and for determining anti-social network activities.

There are other related issues concerning deployment of IEEE 802.11 based network infrastructure for sensor networks that remain to be investigated. The power consumption of IEEE 802.11 based schemes has long been a concern for battery powered systems. Several schemes for reducing IEEE 802.11 power usage at the hardware, protocol and application layer have been reported, however, an integrated study of power reduction techniques over a multi-hop sensor network that includes strong security is needed.

## REFERENCES

- [1] L. Ji, J. Agre, T. Iwao and N. Fujino, "On Providing Secure and Portable Wireless Data Networking Services: Architecture and Data Forwarding Mechanisms", First International Conference on Mobile Computing and Ubiquitous Networking, 2004.
- [2] IEEE, "LAN MAN Standards Of The IEEE Computer Society: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications", IEEE standard 802.11, 1997.
- [3] J. Walker, "Unsafe At Any Key Size; An Analysis Of The WEP Encapsulation.", IEEE 802.11-00/362, 2000.
- [4] W. Arbaugh, N. Shankar, J. Wan, and K. Zhang, "Your 802.11 Network Has No Cloth", Proceedings of the First IEEE International Conference On Wireless LANs And Home Networks, 2001.
- [5] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, 2001.
- [6] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses In The Key Scheduling Algorithm Of RC4", Proceedings of the Eighth Annual Workshop On Selected Areas In Cryptography, 2001.
- [7] Wi-Fi Alliance, "Wi-Fi Protected Access: Strong, standards-based, Interoperable Security for Today's Wi-Fi Networks", Wi-Fi Alliance, ([www.weca.net](http://www.weca.net)), 2003.
- [8] L. Blunk, and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC2284, 1998.
- [9] IEEE, "Port-Based Network Access Control", 2001.
- [10] C. Rigney, W. Willats, and P. Calhoun, "RADIUS Extensions", IETF RFC2869, 2000.
- [11] C. Rigney, W. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)",

IETF RFC2865, 2000.

[12] T. Dierks, and C. Allen, "The TLS Protocol Version 1.0", IETF RFC2246, 1999

[13] J. Kohl, and C. Neuman, "The Kerberos Network Authentication Service (V5)", IETF RFC1510, 1993.

[14] G. Zorn, "Microsoft Vendor-specific RADIUS Attributes", IETF RFC2548, 1999.

[15] IEEE, "Draft Supplement to Standard: LAN MAN Standards Of The IEEE Computer Society: Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", 2002.

[16] IETF, <http://www.ietf.org/html.charters/manet-charter.html>.

[17] H. Luo, et al, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Network", International Conference on Network Protocols, 2001.

[18] L. Zhou, and Z. Haas, "Securing Ad Hoc Networks", IEEE Network, 1999.

## Biography

**Lusheng Ji** is a Research Scientist at the Fujitsu Laboratories of America in College Park, MD. His research interests include ad hoc networks, routing protocols, m-commerce and wireless security. He has a Ph.D. in Computer Science from the University of Maryland where he developed multicast protocols for ad hoc networks.



**Brian Feldman** is a Software Specialist at Fujitsu Laboratories of America in College Park, MD. His research interests include operating systems, wireless protocols, and system security. Prior to Fujitsu he worked on system security at Network Associates. He is currently completing his BS in Computer Science at the University of Maryland.



**Jonathan Agre** is the Director of the Pervasive Computing Department at the Fujitsu Laboratories of America in College Park, MD. His research interests include wireless protocols, sensor networks, m-commerce and performance analysis. He has been involved with various aspects of distributed systems at Jet Propulsion Laboratory, Rockwell Science Center and ARINC Research. He has a BS, MS and Ph.D. in Computer Science from the University of Maryland.

