Suburban Ad-Hoc Networks in Information Warfare

Muhammad Mahmudul Islam, Ronald Pose, Carlo Kopp

Clayton School of Information Technology
Monash University, Australia
{sislam,rdp,carlo}@csse.monash.edu.au

Abstract

Wireless ad-hoc networks are vulnerable partly due to the absence of a clear physical boundary. A simple yet robust network layer security protocol has been proposed previously for Suburban Ad-Hoc Networks. It secures network layer packets at each hop, and provides fully self-organised key and access control management functionalities without relying on any centralised trusted entity. In this paper we extend the possible attack space of SSP. Then we map the possible attacks into the canonical strategies of Information Warfare to evaluate the effectiveness of SSP from the Information Warfare perspective.

Keywords

SAHN, Suburban, Ad-hoc, SSP, Security, Information Warfare

INTRODUCTION

Wireless networks are more vulnerable to various security threats than their wired counterparts. Due to the nature of the wireless media, anyone can eavesdrop and disrupt transmissions with an appropriate transceiver. If the transmitted signals contain unencrypted secret information, eavesdroppers can easily compromise security. If transmitted information is encrypted, security violation may still occur over extended periods if inadequate security schemes are used. For example, if two nodes reuse a shared key over an extended period, an intruder with sufficient computing power may crack the security key using brute force methods. While sophisticated security schemes may be able to reduce attacks from malicious nodes to a satisfactory level, they may be too expensive (in terms of computation and maintenance) and hence impractical to implement. A less sophisticated, yet robust and practically implementable, security scheme is feasible which is capable of containing intrusions, i.e. preventing the damage caused by attackers from spreading through the entire network.

SSP (SAHN Security Protocol) is a simple yet robust security scheme suitable for a SAHN (Suburban Ad-Hoc Network). A SAHN is a multi-hop ad-hoc mesh network proposed by Kopp and Pose (1998) to alleviate the expensive, oversubscribed, area limited and less secured features of existing wireless broadband solutions. SSP secures network layer packets at each hop, and provides fully self-organised key and access control management functionalities without relying on a centralised trusted entity. See Figure 1 for the functional position of SSP in the OSI (Open System Interconnection) model. Since SSP secures network layer packets at each hop, it can prevent the damage caused by the attackers from spreading through the entire network. Simulation results indicate that SSP can perform without compromising the overall network performance. Please refer to (Islam et al., 2004, 2005a) for the simulation results and comparison of SSP with existing security protocols. Note that SSP is an evolution of the previously proposed security protocol for a SAHN known as LLSP (Link layer Security Protocol) (Islam et al., 2004, 2005a).

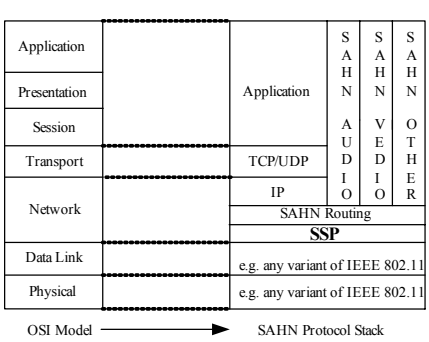
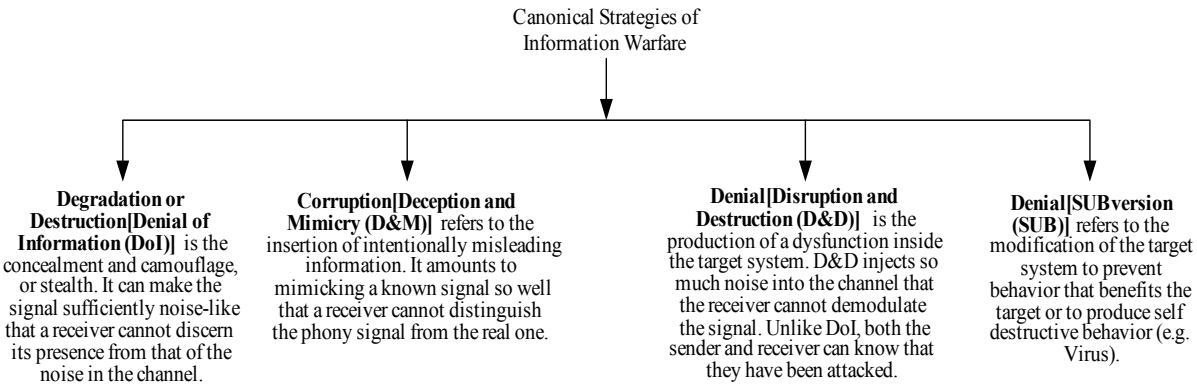


Figure 1: The SAHN protocol stack with SSP in the OSI model.

In this paper we extend the possible attack space that can be handled by SSP. Moreover we map the possible attacks into the canonical strategies of Information Warfare. Figure 2 summarises the four canonical offensive strategies of Information Warfare defined by Kopp (2003). The models for these strategies are depicted in Figures 3. The systematic analysis is beneficial in evaluating the effectiveness of SSP from Information Warfare perspective.



The terms outside the square brackets refer to the actions used by USDoD and the terms within the square brackets refer to the canonical strategies defined by Kopp (2003).

Figure 2: Four canonical offensive strategies of Information Warfare defined by Kopp (2003).

In the next section we discuss related works. Then we briefly describe the working mechanism of SSP. Next we discuss the possible attacks considered for our security protocol. Then we map the possible attack space to the canonical strategies of Information Warfare. Finally we conclude with some plans for future research.

RELATED WORK

SAR (Secure Aware Ad hoc Routing) (Yi et al., 2001) and ARAN (Authenticated Routing for Ad hoc Network) (Sanzgiri et al., 2002, 2005) rely on certification authorities for distributing keys in the network. If a centralised certification authority is used, it has to be online all the time and could be a single point of failure that would make the whole system ineffective. If a distributed certification authority is employed then more than one trusted node would be required to construct a certificate. Depending on the distance in number of hops, the neighbourhood density and the number of the trusted nodes constituting the certification authority, and the update frequency of the keys, the associated communication overhead and response time of getting a reply from the certification authority may not be negligible.

SRP (Secure Routing Protocol) (Papadimitratos and Haas, 2002) does not have intermediate nodes checking the authenticity of route requests and route replies. This means that a malicious node can become part of a routing path and later disrupt the operation of the routing protocol. Its monitoring system may exacerbate greedy behavior of selfish nodes. Moreover it does not protect route error messages. Therefore a malicious node can send false route error messages to isolate a node from the network.

TESLA (Timed Efficient Stream Loss-tolerant Authentication) (Perrig et al., 2000) and Ariadne (Hu et al., 2002b) require nodes to have clock synchronization. They need to buffer packets for authentication that can increase the response time of the routing protocol (Yang et al., 2004).

SEAD (Secure Efficient Ad-hoc Distance vector routing protocol) (Hu et al., 2002a) cannot prevent the ‘same distance attack’ where a malicious node rebroadcasts a route update with the same sequence number and hop count, but with a different sender address.

SADOV (Secure AODV) (Zapta and Asokan, 2002) uses a hash chain like TESLA and Ariadne. A general limitation of a hash chain based approach is that it may be complicated and inefficient for the continual metrics that take non-integer values (Yang et al., 2004).

SLSP (Secure Link State Protocol) (Papadimitratos and Haas, 2003) provides the ‘duplicate MAC address detection’ functionality. Due to this functionality the neighbours of a victim may reject all the link state updates originating from both a malicious node and the victim. Thus a malicious node can succeed in launching a DoS attack against the victim.

Except SAR, none of the above protocols provides any access control mechanism. An access control mechanism can enhance the level of security in a network by assigning different nodes different privileges for accessing different services in the network. All these protocols rely on trusted entities or certification authorities for distributing and managing keys. This reliance should be minimised to reduce the associated communication overhead. Though SSP uses traditional cryptographic primitives, the prerequisites and steps for authentication, key management and access control differ from the above protocols. SSP minimises the shortcomings stated above without incurring too much communication and computational overhead.

OVERVIEW OF SSP

SSP is a password-capability (Anderson et al., 1986) (Castro, 1996) (Kopp, 1997) (Pose, 2001) based security protocol that authenticates per hop communication in a SAHN. A capability is a token that not only identifies an object/resource but also authorises its use (Fabry, 1974). A password capability based system makes access control management simple and robust. The services provided by SSP at each node have been listed in Table 1.

Service	***Invocation***
Authenticate a new neighbor	On demand
Authenticate network membership	On demand
Update encryption/decryption keys	At pseudo random intervals
Reissue capabilities	At pseudo random intervals
Revoke capabilities	On demand
Secure Routing	For every Normal-Packet

*A **Normal-Packet** is a packet sent to SSP by the routing protocol.*

Table 1: *List of services provided by SSP at each node.*

A node *O* in a SAHN can invite any new node *N* to become its neighbour. *N* uses the first service in Table 1 to establish it is an authenticated neighbour of *O*. However, being an authenticated neighbour of *O* does not mean that *N* has become a member of the SAHN. Network membership is needed to communicate with other nodes in the same network. To become a member of the SAHN, *N* has to get a network membership certificate issued by more than one member of the network. With this certificate *N* invokes the second service in Table 1 so that *O* considers *N* as a member of the SAHN and routes its packets. The third and fourth services are needed to update encryption keys and reissue capabilities. The fifth service is required when a node needs to be excluded from the neighbour list or from using the network. The last service in Table 1 is used to secure the routing process at each hop. With all these services SSP builds a secured SAHN where authentication and encryption is performed at each hop, and key and access control management are supported in a fully distributed and self-organised manner.

To authorise *N* to communicate with *O*, *O* issues a capability and a public key to *N*. Here the capability identifies the issuer *O* and the access rights that *O* has given to *N*. *N* has to include this capability in each packet, and sign and encrypt the packet with the public key if it wants *O* to accept the packet for processing at the network layer. *N* has to get the capability and the public key via a secured communication channel.

The initial capability does not permit *N* to send any packet to other nodes in the SAHN through *O*. This capability will be referred to as the Non-Routing-Capability. To get a Routing-Capability from *O,* which will permit *N* to route packets through *O* to other SAHN nodes, *N* has to be authenticated by *O* as a member of the network.

To become a member of the SAHN *N* has to get a certificate issued by more than one member of the network. A fully distributed certification authority (Zhou and Hass, 1999) (Luo and Lu, 2000) can be used for this purpose.

To authenticate network membership, *N* has to send a request to *O* that includes the Non-Routing-Capability and a network membership certificate. If these are valid, *O* issues a Routing-Capability to *N*. If the network membership certificate of *N* is revoked, its Routing-Capability becomes invalid.

A node updates the keys and reissues capabilities given to its neighbours at bounded pseudo random intervals to strengthen the security of SSP.

O also issues a shared key to *N* that is used for signing and encrypting Normal-Packets. A Normal-Packet is a packet sent to SSP by the routing protocol, e.g. a route request or a data packet.

When *N* wants to send a Normal-Packet through *O* to other parts of the network it has to go through SSP's secure routing service. For this service *N* has to include the Routing-Capability that *O* issued in the packet. *N* has to sign and encrypt the packet with the shared key *O* has issued previously. When *O* receives the packet it checks if the signature and the capability are valid. If so the packet is processed according to the routing protocol. Otherwise the packet is dropped.

All these procedures are performed at each node for each of its neighbours. Thus SSP can form a secure SAHN.

POSSIBLE ATTACKS

SSP encrypts the content of each packet in order to protect vulnerable information such as pertaining to routing. Though confidentiality may prevent a malicious node from retrieving information, it can still try to disrupt the normal operation of an ad-hoc network through various attacks, since wireless networks do not have any clear physical boundary. However, the dynamic key management, confidentiality, authentication, integrity and non-repudiation features of SSP can confine the damage so that the attacks cannot spread through the entire network.

In this section we briefly describe the possible attacks that can be prevented by SSP. Interested readers should refer to (Islam et al., 2005a) for the security analysis of SSP with respect to various attacks. It should be noted that SSP is a security protocol that prevents malicious nodes from getting into the system and thus minimises the following attacks. However, SSP cannot prevent a malicious node from jamming the radio channel of a victim node, which is located within the transmission footprint of the malicious node, with noise or storm of traffic. If an authorised node becomes compromised, SSP may not be adequate to ensure security in the network. An intrusion detection system (Islam et al., 2005b) can be used in conjunction with SSP to detect these. Moreover, SSP is unable to thwart a group of malicious nodes from exploiting an ad-hoc network as a communication channel using covert timing channels.

Drop Packets

A malicious node may disrupt the normal operation of a network by dropping packets (Gupte and Singhal, 2003). This type of attack can be classified into two groups:

- *Black-hole attack:* In this type of attack an attacker drops all types of packets.
- *Grey-hole attacks:* Here an attacker selectively drops packets (e.g. only data packets).

Delay Transmissions

A malicious node can give preference in transmitting its own or friends' packets by delaying packets in its output queue. If the packets belong to any time sensitive application, such as real-time video, they may become useless if not received at the receiver in due time.

Protocol Field Modification

A router is supposed to modify various protocol fields in the messages passing through itself according to the associated protocol specification. Existing resource allocation, transmission control or routing protocols are designed on these assumptions. Here are some of the attacks that can be launched by a malicious node exploiting these assumptions to cause disruption in the network.

- *Divert Traffic through Malicious Node:* The path length to a destination in protocols like AODV (Perkins and Royer, 1999) is measured by the hop count field of the route reply packets. A malicious node can advertise a shorter hop count to a destination so by decreasing the actual hop count value in the route reply packet. Thus it succeeds in diverting all the traffic for that destination through itself (Sanzgiri et al., 2002).

  Since the malicious node has become part of the routing path, it can do anything with the packets diverted to it. It can drop or delay packets.

- *Divert Traffic through Endless Loop:* Protocols like DSR (Johnson and Maltz, 1996) require the inclusion of the list of intermediate nodes in each packet, known as source route, for routing packets. A malicious node can become part of the routing process and modify the source route to create loops

(Sanzgiri et al., 2002). Consequently it can succeed in launching a DoS attack against the destination of the route since the destination will not receive the packets.

- *Divert Traffic through Bottleneck Node:* A QoS protocol may send probe packets along a set of possible paths for a particular destination to gather information about how much bandwidth is available along each path. The path having the most bandwidth available may be selected as a new route. A QoS protocol usually assumes that the nodes, which are on the routing path, set the fields in the probe packets. Moreover, a node is not supposed to modify a value that has been set by another node.

  If a malicious node becomes an intermediate node of any of the paths that do not have enough bandwidth available for the new flow, it can increase the available bandwidth values set by other nodes in such a way that the path will ultimately be selected as the routing path for the new flow. When traffic starts to flow the selected path, it is very likely that all the flows passing through the bottleneck node/nodes will be impeded and hence the overall network performance will degrade.

Message Fabrication

Sanzgiri et al. (2002) have defined message fabrication as the generation of false routing messages. However, we have redefined this term to expand its scope. That is, in our work message fabrication would imply the generation of any (except for the MAC (Medium Access Control) control messages) false control message. Message fabrication can take any of the following forms:

- *Divert Traffic through Malicious Node:* We have already discussed this type of attack previously that occurs when a malicious node becomes part of the route reply paths and makes changes in the routing protocol fields. Here we present others ways that a malicious node may use to divert traffic through itself. We will explain these mechanisms in terms of DSR.

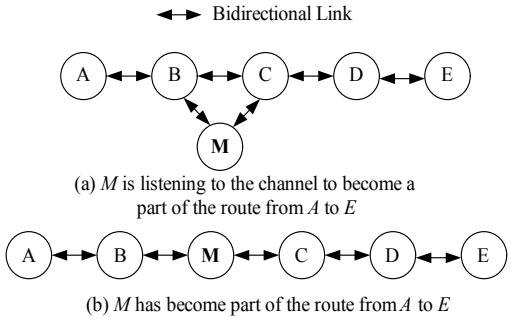


Figure 3: The *malicious node M is becoming a part of the routing path from A to E.*

Nodes in DSR learn new routes by overhearing transmissions from neighbouring nodes. A malicious node can use this vulnerability to announce false routes that are shorter than existing routes to redirect traffic through itself. For example (see Figure 3), a malicious node *M* can transmit spoofed packets with a shorter source route *E* via itself. *B* may add this route to its route cache and divert all traffic, destined for *E*, to *M*. Thus *M* becomes part of the routing path and can drop or delay subsequent data packets. This particular attack is also known as 'Route Cache Poisoning' (Sanzgiri et al., 2002).

- *Force Termination of Ongoing Flows:* Some routing protocols, such as AODV and DSR, facilitate route maintenance by sending error messages from the nodes preceding broken links. Since these messages are not authenticated in traditional AODV or DSR, a malicious node can send a false error message against a working node *W* so that the source node, sending packets to a destination through *W*, deletes its corresponding route entry (Sanzgiri et al., 2002). If the source node does not have any other route to the destination, the malicious node can succeed in launching a DoS attack by stopping the ongoing traffic towards that destination.
- *Routing Table Overflow:* A node can contain a finite number of route entries in its route table. In reactive routing protocols, a malicious node can try to overflow route tables of other nodes by initiating route discovery for non-existent nodes (Sanzgiri et al., 2002). In proactive routing, the same purpose can be achieved by broadcasting route information of non-existent nodes (Sanzgiri et al., 2002). In this way the malicious node can prevent other nodes adding legitimate route entries in their route tables.

- *Denouncing a Benign Node:* A malicious node can report to other nodes of the network that a benign node is misbehaving. If the report is not authenticated, the benign node may not get any legitimate service from other members of the network.

Replay Attack

In this attack a malicious node intercepts a message and retransmits it at a later time modified or unmodified. By replaying stale information the malicious node can cause inconsistency in the network and consequently can prevent the network from operating properly. A repetitive replay attack can blind a target node with storm of traffic so that other nodes are prevented from getting any service from the attacked node.

Broadcast Storm Attack

A malicious node can send network wide broadcast packets to a node within its transmission range. If the packets are not authenticated, the node will rebroadcast the packet to its neighbourhood. If this process continues, the whole network can be flooded with so much traffic that transmission contention (if the network uses a contention based MAC protocol) and network congestion may become inevitable. Consequently legitimate flows may not be able to get their required QoS.

Piggyback Attack

If a malicious node knows how packets are routed in a network, it can piggyback its messages on network-wide broadcast packets to send it to its accomplice located on other part of the network. If the malicious node sends a large number of packets within a short time period, the network may face the problems similar to the broadcast storm attack. Figure 4 illustrates a piggyback attack.

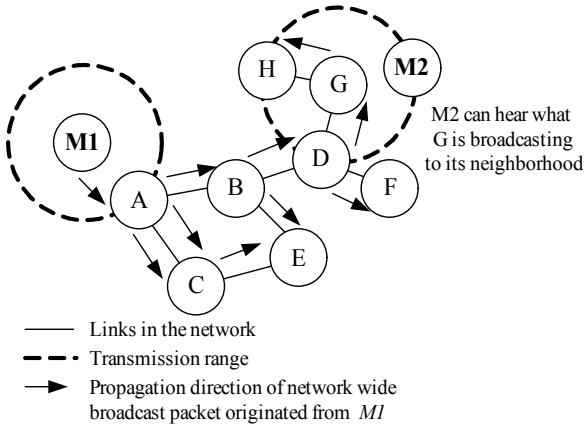


Figure 4: *Piggyback attack where a malicious node M1 is using the network as a carrier for sending messages to another malicious node M2.*

Tunnelling Attack

This is also known as the 'Wormhole Attack' (Hu et al., 2003). In this attack one or more malicious nodes link two parts of a network through a path that may seem shorter in distance or duration than would otherwise be expected (Sanzgiri et al., 2002). This attack does not require the malicious nodes to have any knowledge of cryptographic keys (Gupte and Singhal, 2003). The results of this attack could be diverting traffic through malicious nodes or preventing nodes from discovering paths more than a certain length.

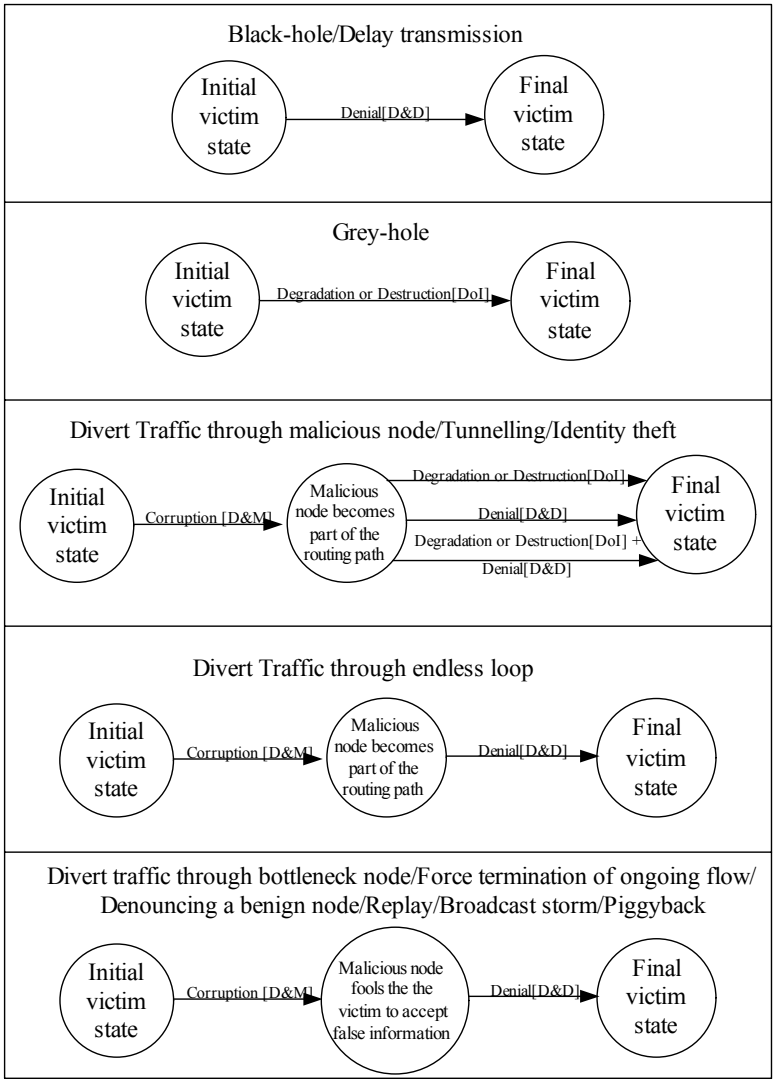
Identity Theft

In the absence of any authentication mechanism a malicious node can easily masquerade as a legitimate node by changing its identity (e.g. IP and MAC addresses) to that of the legitimate node (Sanzgiri et al., 2002). In this way the malicious node can perform any of the attacks mentioned so far without being detected.

MAPPING POSSIBLE ATTACKS INTO THE CANONICAL STRATEGIES

Information warfare attacks in practice most frequently involve compound strategies. Hence the possible attacks, described in the previous section, comprise one or more of the four canonical strategies. It should be noted that each of the canonical strategies is atomic. Therefore any compound strategy can be divided into a number of canonical strategies but a canonical strategy cannot be further divided in any way (Kopp, 2005).

We now show how each of the possible attacks maps into the four canonical strategies of Information Warfare (Kopp, 2003). To do this we attempt to fit each of the possible attacks in any of the four canonical strategies. If there is no direct match, we can start with an initial state and generate a series of states to reach the final state where a transition from one state to another is indicated by an atomic or compound strategy. The state transition diagrams in Figure 5 shows that most of the possible attacks map into more than one canonical strategy.



The terms outside the square brackets refer to the actions used by United States Department of Defense and the terms within the square brackets refer to the canonical strategies defined by Kopp (2003).

Figure 5: *State transition diagrams of the possible attacks.*

Possible Attacks \ Canonical Information Warfare Strategies	Degradation or Destruction[DoI]	Corruption[D&M]	Denial[D&D]	Denial[SUB]
Black-hole			X	
Grey-hole	X			
Delay Transmissions			X	
Divert Traffic Through Malicious Node (Protocol Field Modification)	X	X	X	
Divert Traffic Through Endless Loop		X	X	
Divert Traffic Through Bottleneck Node		X	X	
Divert Traffic Through Malicious Node (Message Fabrication)	X	X	X	
Force Termination of Ongoing Flows		X	X	
Routing Table Overflow		X	X	
Denouncing a Benign Node		X	X	
Replay		X	X	
Broadcast Storm		X	X	
Piggyback		X	X	
Tunnelling	X	X	X	
Identity Theft	X	X	X	

The terms outside the square brackets refer to the actions used by United States Department of Defense and the terms within the square brackets refer to the canonical strategies defined by Kopp (2003).

Table 2: *Mapping of the possible attacks into the Information Warfare strategies.*

A piggyback attack may not degrade the network performance if the associated malicious nodes do not overload the network with excess traffic. The intention of the malicious nodes may be only to exploit the network as a carrier for their unauthorised traffic. In that case, the final state of the piggyback attack cannot be considered as Denial[D&D] anymore. However Corruption[D&M] would still be considered as a preamble for the piggyback attack.

Table 2 summarises the Figure 5 in tabular form. It is clear that the current attack space of SSP does not include the Denial[SUB] strategy. Therefore, though SSP can be expected to be effective against most of the offensive canonical strategies, it may not be able to prevent an attack comprising the Denial[SUB] strategy. This area needs to be considered carefully to make necessary improvements in SSP to increase its effectiveness.

CONCLUSION

We have extended the possible attack space for SSP. Then we have analysed the possible attacks with state transition diagrams to map them to the four canonical offensive strategies of Information Warfare. This study suggests that the SUB strategy needs to be considered in the attack space to enhance the effectiveness of SSP. In the future we plan to address this issue. We also want to make SSP effective against covert timing channel attacks and integrate SSP with an intrusion detection system.

REFERENCES

Anderson, M., Pose, R., and Wallace, C.S. (1986). A Password-Capability System, *The Computer Journal,* **29**, 1: 1-8.

Castro, M. D. (1996). The Walnut Kernel : a password-capability based operating system. Ph.D. Thesis, Monash University, Clayton, Australia.

Fabry, R. S. (1974). Capability-based addressing, *Communications of the ACM* **17**(7): 403–412.

Gupte, S. and Singhal, M. (2003). Secure routing in mobile wireless ad hoc networks, *Elsevier* **1**(1): 151–174.

Hu, Y.-C., Johnson, D. B. and Perrig, A. (2002a). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, *4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 3-13.

Hu, Y.-C., Perrig, A. and Johnson, D. B. (2002b). Ariadne: A secure on-demand routing protocol for ad-hoc networks, *8th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 23-28.

Hu, Y.-C., Perrig, A. and Johnson, D. (2003). Packet leashes: a defense against wormhole attacks in wireless networks, *INFOCOM*, Vol. 3, IEEE, pp. 1976–1986.

Islam, M. M., Pose, R. and Kopp, C. (2004). A Link Layer Security Protocol for Suburban Ad-Hoc Networks, *Australian Telecommunication Networks and Applications Conference (ATNAC)*.

Islam, M. M., Pose, R. and Kopp, C. (2005a). Link Layer Security for SAHN Protocols, *IEEE PerCom Workshops on PWN*.

Islam, M. M., Pose, R. and Kopp, C. (2005b). An Intrusion Detection System for Suburban Ad-hoc Networks, *To appear at the IEEE Tencon*.

Johnson, D. and Maltz, D. (1996). *Dynamic Source Routing in Ad-hoc Wireless Networks*, chapter 5, pp. 153–81.

Kopp, C. (1997). An I/O and stream inter-process communications library for a password capability system. MS Thesis, Monash University, Clayton, Australia.

Kopp, C. (2003). Shannon, Hypergames And Information Warfare, *Journal of Information Warfare*, **2**, 2: 108-118.

Kopp, C. (2005). The Analysis of Compound Information Warfare Strategies. *To appear at the 6th Australian Information Warfare and Security Conference.*

Kopp, C. and Pose, R. (1998). Bypassing the Home Computing Bottleneck: The Suburban Area Network, *3rd Australasian Computer Architecture Conference*, pp. 87–100.

Luo, H., and Lu, S. (2000). Ubiquitous and robust authentication services for ad hoc wireless networks*, Technical Report TR-200030*, Department of Computer Science, UCLA.

Papadimitratos, P. and Haas, Z. J. (2002). Secure Routing for Mobile Ad Hoc Networks, *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*.

Papadimitratos, P. and Haas, Z. J. (2003). Secure Link State Routing for Mobile Ad Hoc Networks, *Symposium on Applications and the Internet Workshops (SAINT)*, pp. 27-31.

Perkins, C. and Royer, E. (1999). Ad-hoc On-Demand Distance Vector Routing, *2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100.

Perrig, A., Canetti, R., Tygar, J.D. and Song, D. (2000). Efficient Authentication and Signing of Multicast Streams over Lossy Channels, *IEEE Symposium on Security and Privacy*, pp. 56-73.

Pose, R. (2001). Password-capabilities: their evolution from the password-capability system into walnut and beyond, *in* G. Heiser (ed.), *6th Australasian Computer Systems Architecture Conference (ACSAC)*, Vol. 23, IEEE Computer Society Press, pp. 105–113.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21**(2): 120–126.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C. and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks, *10th IEEE International Conference on Network Protocols*, pp. 78-89.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C. and Belding-Royer, E. M. (2005). Authenticated Routing for Ad Hoc Networks, *IEEE Journals on Selected Areas in Communications,* **23**(3): 598-610.

Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004). Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications,* **11**(1): 38-47.

Yi, S., Naldurg, P. and Kravets, R. (2001). Security-aware ad hoc routing for wireless networks, *ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*.

Zapata, M. G. and Asokan, N. (2002). Securing Ad Hoc Routing Protocols, *ACM Workshop on Wireless Security (WiSe),* pp. 1-10.

Zhou, L., and Hass, Z. J. (1999). Securing Ad Hoc Networks. *IEEE Networks*, **13**, 6: 24-30.

COPYRIGHT