J. Indian Inst. Sci., July–Aug. 2006, **86**, 397–405

Secured power aware virtual node routing scheme for ad-hoc networks

A. KUSH[1,]*, R. KUMAR[1] AND P. GUPTA[2]
[1]Department of Computer Science, Kurukshetra University, Kurukshetra 136 119, India.
emails: {akush20,rkckuk}@rediffmail.com; Phone: 01-184-2204087, 919896210014.
[2]Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur 208 016, India. email: pg@cse.iitk.ac.in.

Received on June 3, 2005; Revised on March 2, 2006.

Abstract

A recent trend in ad-hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most protocols in this category do not incorporate proper security features. The ad-hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. The proposed scheme is intended to be incorporated on the power aware virtual node routing protocol to protect its routing strategy. The study will help in making protocol more robust against attacks and standardizing parameters for security in routing protocols.

Keywords: Security, ad-hoc networks, routing protocols, secure PAVNR.

1. Introduction

An ad-hoc wireless network is a collection of mobile devices equipped with interfaces and networking capability. It is adaptive in nature and is self-organizing. A formed network can be de-formed and again formed on the fly and this can be done without the help of system administration. Each node may be capable of acting as a router. Applications include but are not limited to virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files, etc. Although security has long been an active research topic in wired networks, the unique characteristics of ad-hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Consequently, the existing security solutions for wired networks do not directly apply to the ad-hoc environment. The main goal of the security solutions for an ad-hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1]. One distinguishing characteristic of this network from the security design perspective is the lack of a clear line of defense. Unlike

*Author for correspondence.

Table I
Secure routing

Security problem	Technique
Timeliness	Timestamp
Authenticity	Password, certificate
Integrity	Digital signature
Confidentiality	Encryption
Ordering	Sequence number

wired networks that have dedicated routers, each mobile node in an ad-hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In such an environment, there is no guarantee that a path between the two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. A new scheme has been proposed here to incorporate security features in ad-hoc networks. The scheme takes care of basic security needs and uses concept of hash key generation to attain the goal of security. The scheme has been incorporated on the refined version of AODV [2], named as PAVNR [3] called power aware virtual node routing protocol. PAVNR embeds the function of power and virtual nodes factor in AODV and improves its performance to achieve more stable routes. Rest of the paper is organized as follows: Section 2 describes the types of security attacks: related work is described in Section 3, Section 4 is the proposed scheme, Section 5 deals with security model with its impacts and Section 6 concludes the study.

2. Security attacks

General solution to the security attacks can be from traditional approaches as described in Table I. In this paper, the prime concern is with the attacks targeting the routing protocols for ad-hoc networks. These attacks can be broadly classified into two main categories as: Passive attacks, and active attacks.

2.1. *Passive attacks*

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. The attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes, or which nodes are pivotal to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring down the network. The nature of attacks varies greatly from one set of circumstances to another. Some of the generic types of attack [4, 5] that might be encountered in passive attacks are:

1. Interruption: An asset of the system is destroyed, becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, or cutting of a communication line.
2. Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Examples include wiretapping to capture data in a network or the illicit copying of files.

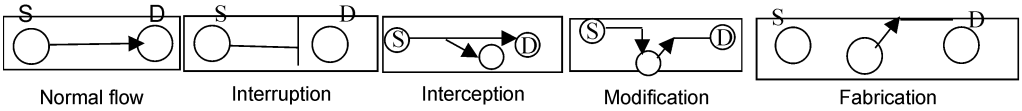


FIG. 1. Types of passive attacks. S represents source and D represents destination.

3. Modification: An unauthorized party tampers with an asset. This is an attack on integrity. Examples include changing values in a data file or modifying the contents of a message being transmitted in a network.
4. Fabrication: An unauthorized party inserts malicious objects into the system. This is an attack on authentication. Examples include the insertion of spurious messages in a network or the addition of records to a file (Fig. 1).

2.2. *Active attacks*

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories.

1. Replacement: In this attack one entity pretends to be a different entity. A type of attack that is used by someone familiar with your security procedures and failures. An impersonate attack usually includes one of the other forms of active attacks.
2. Replay: This involves capture of data units and its subsequent retransmission to produce an unauthorized effect. Sniffers are used for legitimate network management functions.
3. Modification of messages: This simply means that some portion of a legitimate message is altered, delayed or reordered. Someone between you and your connection works as an intermediary, listening in on your communications and possibly modifying them.
4. Denial of service: This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. It is like shutting down a server that could not otherwise be compromised.

It is quite difficult to prevent active attacks absolutely, as this would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them (Fig. 2).

3. Related work

Despite the fact that security of ad-hoc routing protocols is causing a major roadblock in commercial application of this technology, only a limited work has been done in this area.

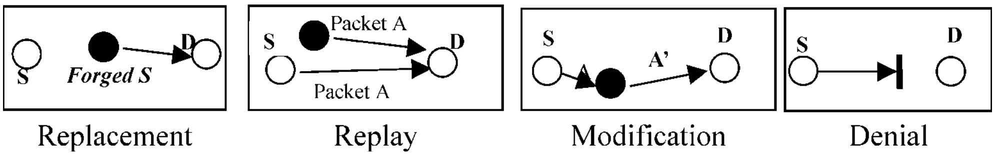


FIG. 2. Types of active attacks. S represents source and d, destination.

Such efforts have mostly concentrated on the aspect of data forwarding, disregarding the aspect of topology discovery. On the other hand, solutions that target route discovery have been based on approaches for fixed-infrastructure networks, defying the particular ad-hoc network challenges. Dahill *et al.* [6] proposed ARAN. It assumes managed open environment, where there is a possibility for predeployment of infrastructure. It consists of two distinct stages. The first is the certification and end-to-end authentication stage. Here the source gets a certificate from the trusted certification server, and then using this certificate, signs the request packet. Each intermediate node in turn signs the request with its certificate. The destination then verifies each of the certificates, thus the source gets authenticated and so do the intermediate nodes. The destination node then sends the reply along the route reverse to the one in the request, reply signed using the certificate of the destination. The second stage is a non-mandatory stage used to discover the shortest path to the destination, but this stage is computationally expensive. It is prone to reply attacks using error messages unless the nodes have time synchronization. Papadimitratos and Haas [7] proposed a protocol (SRP) that can be applied to several existing routing protocols. This protocol assumes a security association between source and destination nodes. Intermediate nodes do not need to cryptographically validate the control traffic. It adds an SRP header to the base routing protocol (DSR or AODV) request packet. SRP header has three important fields—QSEQ which helps prevent replay of old outdated requests, QID and random number which helps prevent fabrication of requests, and an SRP MAC which ensures integrity of the packets in transit. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. ARIADNE [8] is based on DSR [9] and TESLA [10] (on which its authentication mechanism is based). ARIADNE prevents attackers/compromised nodes from disrupting uncompromised routes comprising benign nodes. It uses highly efficient symmetric key cryptography. ARIADNE does not guard against passive attackers eavesdropping on the network traffic. It does not prevent an attacker from inserting data packets. It is vulnerable to active-1-1 attacker that lies along the discovered route, which does not forward packets and does not generate ERROR if it encounters a broken link. It also requires clock synchronization, which we consider to be an unrealistic requirement for ad-hoc networks. Perlman proposed a link state routing protocol [11] that achieves Byzantine robustness. Although the protocol is highly robust, it requires a very high overhead associated with public key encryption. In their paper on securing ad-hoc networks, Zhou and Haas [12] primarily discuss key management. They devote a section to secure routing, but essentially conclude that “nodes can protect routing information in the same way they protect data traffic”. They also observe that denial-of-service attacks against routing will be treated as damage and routed around. Some work has been done to secure ad-hoc networks by using misbehavior detection schemes [13, 14]. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving; and second has no real means to guarantee the integrity and authentication of the routing messages.

Looking at the work that has been done in this area previously, it seems that the security needs for ad-hoc networks have not been yet satisfied. Also, ad-hoc networks services are provisional and batteries are a limited resource.

4. Proposed scheme

Efforts have been made to incorporate the proposed model on AODV with already added features of power and virtual nodes in the protocol PAVNR [3], which uses the concept of power awareness among route selection nodes and concept of virtual nodes which insures fast selection of routes with minimal efforts and faster recovery. Working of the PAVNR can be described in three phases as route construction, route maintenance and local route repair.

4.1. *Route construction*

This scheme can be incorporated with reactive routing protocols that build routes on demand via a query and reply procedure. The algorithm works by sending a RREQ (route request) propagation process when a source needs to initiate a data session to a destination but does not have any route information; it searches a route by flooding a ROUTE REQUEST (REQ) packet. Each REQ packet has a unique identifier so that nodes can detect and drop duplicate packets. An intermediate node with an *active route* (in terms of power and virtual nodes), upon receiving a no duplicate REQ, records the previous hop and the source node information in its route table, i.e. backward learning. It then broadcasts the packet or sends back a ROUTE REPLY (REP) packet to the source if it has an *active route* to the destination. The destination node sends a REP via the selected route.

4.2. *Route error and maintenance*

When the node detects a link break, it performs a one hop data broadcast to its immediate neighbors. The node specifies in the data header that the link is disconnected and thus the packet is candidate for alternate routing. Upon receiving this packet, route maintenance phase starts by selecting alternate path with virtual nodes and checking power status.

4.3. *Local route repair*

When a link break in an active route occurs, the node upstream of that break may choose to repair the link locally if the destination was no farther and there exist virtual nodes (VN) that are active. To repair the link break, the node increments the sequence number for the destination and then broadcasts a REQ for that destination. The time to live (TTL) of the REQ should initially be set to the following value

$$\text{TTL} = \max\,(\text{VN attached}, 0.5 * \#\text{hops}) + \text{POWER status},$$

where #hops is the number of hops to the sender (originator) of the currently undeliverable packet. Power status is checked from route table, VN attached is the number of virtual nodes attached. This factor is transmitted to all nodes to select best available path with maximum power. Thus, local repair attempts will often be invisible to the originating node. To carry out the study on PAVNR, several attacks that can occur on PAVNR and existing reactive protocols have been identified as:

4.3.1. *External attacks in PAVNR*

1. Routing table inconsistencies: A malicious node impersonates another node and sends routing updates. False route requests, replies and updates could cause inconsistencies in the routing table.

2. Wrong routing: Tampering of control messages, which could result in incorrect route information.
3. Denial of service: This can be done generating false broadcast packets like route requests. The network can be flooded with wasteful packets thereby preventing channel access to rightful users.

4.3.2. *Internal attacks in PAVNR*

1. Generation of false messages: This could be done by generation of false control messages like route requests. It is extremely difficult to differentiate between a misbehaving node and a node that genuinely needs to establish routes to many other nodes.
2. Data tampering: A compromised node could tamper with information and cause havoc in the network.
3. Not forwarding packets: Not forwarding data/control packets could cause considerable damage.
4. Sending false replies: An intermediate node that does not have a route to the destination can falsely reply, thereby causing discovery of wrong routes.
5. Forwarding packets to incorrect nodes: If a packet is forwarded to an incorrect node, the packet may either never reach the destination or the path it takes might be a very costly one.

5. Security model

Most previous work on secure ad-hoc network routing relies on asymmetric cryptography such as digital signatures [12–15]. However, computing such signatures on resource-constrained nodes is expensive, and it is assumed that nodes in the ad-hoc network may be so constrained. As a general design principle, a node trusts only itself for acquiring information about which nodes in the network are malicious. In general, ad-hoc network routing protocols do not need secrecy or confidentiality. These properties are required to achieve privacy or anonymity for the sender of messages. The proposed scheme has taken into account the following design criteria as to achieve complete security in terms of availability, integrity and authentication, minimal overhead, network performance in terms of throughput and node mobility.

The proposed scheme is based on the hash key chain mechanism. Hash key chains are constructed by using only symmetric cryptographic primitives, namely, hash functions. Authentication and integrity can be achieved by using hash key chains. A hash key chain is configured as a recursive chain, where the node first chooses a random key, K_1. Subsequent keys are calculated by calculating the one-way hash over the key:

$$K_2 = H[K_1],\ K_{N-2} = H[K_{N-1}],\quad K_{N-1} = [K_N]\ \ldots$$

To compute any previous key from key K_I where $J < \mathrm{I}$ a node uses the equation: $K_j = H_{I-J}$ $[K_I]$.

This equation is used by any node to authenticate any received value on the hash chain. If the computed value matches previous known authentic key value then the received key is authentic. Each node discloses each key of its one-way key chain in a particular order, which is exactly reverse of the order in which the keys were generated. The key disclosure schedule and key generation schedule should be reverse For example, if the keys were generated by a node in the order K_N; K_{N-1}; … K_1; K_0 then the node discloses them in the order K_0; K_1; … K_N. The rationale behind having the key disclosure schedule to be reverse of the key generation schedule is that K_N of a node is known to all other nodes and in such a situation they should be able to authenticate any subsequent keys that are disclosed. The use of one way hash function allows K_0; K_1; … K_{N-1} to be authenticated using K_N but K_N cannot be authenticated using any other key value. Hence the key disclosure schedule and key generation schedule is reverse. The scheme was proposed earlier by Lamport [16]. Hashing is done for route request, reply and local route repair and not in route error and route erasure phases so that less overhead occurs. If in REQ phase if intermediate node cannot satisfy the security requirements, the REQ packet is dropped and not forwarded. Some mobile nodes will be compromised during the operation. Arrival of REQ to destination will ensure a safe path. REP packet contains this security information specified by sender. So an additional field is added to REQ and REP packet formats. This scheme will be able to take care of external attacks. In order to check internal attacks, some of the techniques that can be used are: Flooding of packets for false route requests, false route replies and also using one way hash to achieve objectives of tampering can be done to take care of internal attacks. As is evident from the proposed scheme, the format size will be increased with inclusion of hash key generation. The routing load will increase due to incorporation of security. It is also clear that the scheme affects the packet delivery fraction and end-to-end delay. The packet delivery fraction will be marginally reduced. Also chances of packets drop may increase due to delay produced in route reply case. This could be improved by having higher timeouts for packets buffered for route discovery. Changed formats compared with AODV and PAVNR are described in Appendix I.

6. Simulation results

Simulation study has been carried out to study the performance of the proposed protocol. Simulation environment used for this study is NS 2.26 [17]. Figure 3 shows the packet delivery ratio based on pause time. The packet delivery ratio is the fraction of successfully received packets, which survive while finding their destination. This performance measure determines the completeness and correctness of the routing protocol. Pause time of 0 means very fast moving nodes and 500 shows minimum movement.

As the figure shows secured PAVNR has less number of packets delivered, but this reduction in delivery is due to hash keys calculations and evaluations. Figure 4 represents the end-to-end delay with respect to pause time. Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. This is a good metric for comparing protocols and denotes how efficient the underlying routing protocol is, because delay primarily depends on optimality of path chosen. More end-to-end delay is observed in this case for secured PAVNR. The reason again is the calculation part involved for hash key estimation. It should be noted here that only trusted packets are delivered, so some packets do fall because of this reason also.

The reduction in packet delivery ratio and increase in end-to-end delay does not show the effectiveness of the proposed scheme. This change will be obvious as more packets are sac

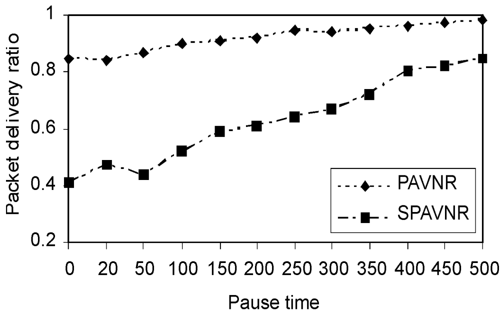


FIG. 3. Packet delivery ratio (50 nodes).

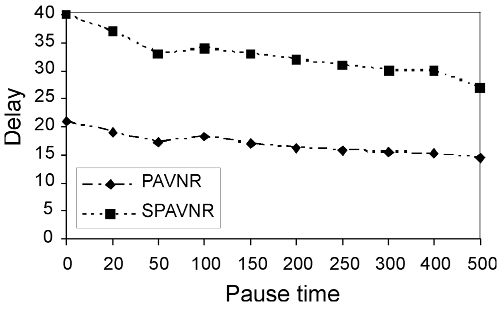


FIG. 4. End-to-end delay.

rificed to keep them secured. Security is achieved at the cost of performance. Efforts are on to reduce the margins by reducing the size of hash key.

6. Conclusion

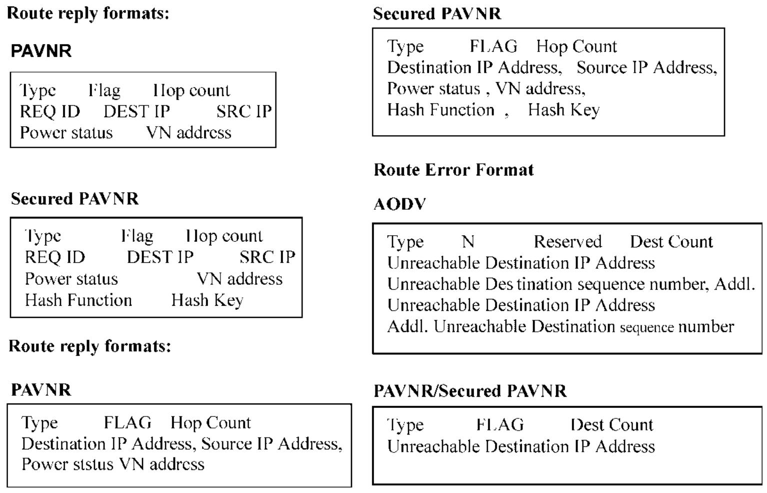
An analytical study has been done for contemporary secured routing protocols for ad-hoc networks. Areas have been identified where further work can be done. A new solution has been proposed as hash key generation. It is clear that different protocols will have different solutions. In this paper the emphasis is on PAVNR and it is further suggested that the approach can be utilized in DSR also. The idea has been conceptualized in Hu *et al.* [8] for DSR. Hash key management is one of the best options, though other options can also be considered depending upon the need of security. As hash key chain is configured as a recursive chain so these keys are noted in route table. This increases memory requirements but hash key management is efficient as it does not involve any additional packet overhead. Important function is that the routing protocol functions very similar to the existing one when there are no external attacks. Whenever an attack occurs additional packets need to be sent to change the routes established by the malicious control packets. This increased traffic size will have its impact on overhead. The overhead is bound to increase with it, but keeping in view of the better secured routing this will have to be done to achieve the desired results. Efforts are on to simulate the proposed scheme with different topologies and compare it with existing secured routing schemes. The proposed scheme is expected to work better in dense environments as selection of path becomes easy in case of failures. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad-hoc network security is to develop a multifence security solution that is embedded possibly into every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats.

References

1. R. Hauser, A. Przygienda, and G. Tsudik, Reducing the cost of security in link state routing. In *Symp. Network and Distributed Systems Security* (NDSS '97), San Diego, California, pp. 93–99, 1997, Internet Society.

2. C. Parkins, and E. Royer, Ad-hoc on demand distance vector routing, *2nd IEEE Workshop on Mobile Computing*, pp. 90–100 (1999).
3. A. Pandey, P. Gupta, A. Kush, and C. J. Hawang, Power aware virtual node routing scheme in ad-hoc networks, *IASTED Int. Conf. on Wireless Networks and Emerging Technologies* (WNET 2004), Banff, Canada, pp. 698–704 (2004).
4. T. Karygiannis, and L. Owens, *Wireless network security*, NIST Special Publication 800-48 (2002).
5. Yonguang Zhang, and Wenke Lee, Intrusion detection in wireless ad-hoc networks, *6th Int. Conf. on Mobile Computing and Networking* (MOBICOM'00), pp. 275–283 (2000).
6. B. Dahill, B. N. Levine, E. Royer, and C. Shields, *A secure routing protocol for ad-hoc networks*, Technical Report UM-CS-2001-037, Department of Computer Science, University of Massachusetts (2001).
7. P. Papadimitratos, and Z. J. Haas, Secure routing for mobile ad-hoc networks, *SCS Communication Networks and Distributed Systems Modeling and Simulation Conf.* (*CNDS 2002*) (2002).
8. Y. C. Hu, A. Perrig, and D. Johnson, *ARIADNE: A secure on-demand routing protocol for ad-hoc networks*, Technical Report TR01-383, Rice University (2001).
9. D. B. Johnson *et al.*, *The dynamic source routing protocol for mobile ad-hoc networks (DSR)*, Internet draft, MANET Working Group (2002).
10. A. Perrig, R. Canetti, D. Song, and D. Tygar, Efficient and secure source authentication for multicast, In *Network and Distributed System Security Symposium (NDSS'01)* (2001).
11. R. Perlman, Fault-tolerant broadcast of routing information, *Computer Networks*, **7**, 395–405 (1983).
12. L. Zhou, and Z. J. Haas, Securing ad-hoc networks, *IEEE Network Mag.*, **13**, 24–30 (1999).
13. S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad-hoc networks, In *Proc. Sixth Annual Int. Conf. Mobile Computing and Networking*, pp. 255–265 (2000).
14. William Stallings, *Cryptography and network security: Principles and practice*, Second edition, pp. 3–12, Prentice Hall (2001).
15. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM*, **21**, 120–126 (1978).
16. L. Lamport, Password authentication with insecure communication, *Commun. ACM*, **24**, 770–772 (1981).
17. NS Notes and documentation, available at www.isi.edu/vint.

Appendix 1



Route reply formats:

PAVNR

Type Flag Hop count
REQ ID DEST IP SRC IP
Power status VN address

Secured PAVNR

Type Flag Hop count
REQ ID DEST IP SRC IP
Power status VN address
Hash Function Hash Key

Route reply formats:

PAVNR

Type FLAG Hop Count
Destination IP Address, Source IP Address,
Power ststus VN address

Secured PAVNR

Type FLAG Hop Count
Destination IP Address, Source IP Address,
Power status , VN address,
Hash Function , Hash Key

Route Error Format

AODV

Type N Reserved Dest Count
Unreachable Destination IP Address
Unreachable Des tination sequence number, Addl.
Unreachable Destination IP Address
Addl. Unreachable Destination sequence number

PAVNR/Secured PAVNR

Type FLAG Dest Count
Unreachable Destination IP Address