A Key Management Solution for Secure Routing in Mobile Ad Hoc Networks

Sulaiman ASHRAPH
asulaiman@nur.ac.rw
National University of Rwanda
Butare, Rwanda

and

Dawoud S DAWOUD
dshenouda@nur.ac.rw
National University of Rwanda
Butare, Rwanda

and

Adronis NIYONKURU
aniyonkuru@nur.ac.rw
National University of Rwanda
Butare, Rwanda

ABSTRACT

This paper investigates the need for security and more specifically key management for secure routing in mobile ad hoc networks. A key management protocol is proposed for on-demand ad hoc routing protocols. The proposal provides key distribution and security evaluation to allow the most secure path to be selected during route discovery. Simulations modeled in ns-2 investigate the success of the key distribution mechanism and security scheme.

Keywords: Ad hoc networks, Trust chain, On-demand routing protocol, Secure Routing.

1. INTRODUCTION

With recent wireless technology advances mobile ad hoc networks have found increasing application in the military and commercial domain. However the unique characteristics of mobile ad hoc network make them difficult to secure. Such characteristics include the lack of network infrastructure, no prior relationships, unreliable multi-hop communication channels, resource limitation and node mobility. Before these dynamic networks can be deployed into the commercial and military arena they must be secured against malicious attackers.

We identify that most of the security attacks target the network layer and more specifically the routing protocol. Such attacks include blackhole attacks, wormhole attacks, eavesdropping attacks, byzantine attacks, resource consumption attacks and routing table poisoning. The network layer provides a critical service to the mobile ad hoc network, called the routing protocol. In the context of trust and security the provision of secure routes is one of the most vital elements for trust establishment. Adversaries target the routing protocol specifically and a secure routing solution is needed for a secure implementation and deployment of ad hoc networks.

Secure ad hoc routing protocols exist but their operational assumptions typically include an existing key management system. The following section investigates the operational requirements for existing secure ad hoc routing protocols. Secure ad hoc routing protocols are divided into three categories: symmetric cryptography, asymmetric cryptography, and reputation based protocols.

Although symmetric cryptographic approaches do not rely on a public key infrastructure they still require some kind of key management in an ad hoc network. The SEAD protocol [1] designed for the table-driven DSDV routing protocol requires a key management mechanism to distribute an authenticated initial hash element. SEAD uses a one-way hash function to provide hop-by-hop authentication for routing packets hop count and sequence numbers. Ariadne [2] proposed a DSR based on-demand protocol uses TESLA authentication [3] to provide end-to-end authentication. A key management system is assumed present to distribute the TESLA keys. TESLA authentication also requires clock synchronization between participating nodes which is difficult without the presence of an online TTP.

ARAN [4], SAODV [5] and SLSP [6] use asymmetric cryptography and key management is simply assumed for each of these protocols. ARAN assumes that an online TTP is present that acts as a certificate authority (CA) to provide end-to-end authentication in an on-demand environment. Prior shared secrets are assumed between all participating nodes and the CA. The SAODV protocol is based on the AODV on-demand routing protocol and provides end-to-end authentication by authenticating the routing packets' mutable fields with a hash chain and immutable fields with a digital signature [5]. SAODV assumes the presence of a key management system to distribute keys and initial hash elements. SLSP secures a table driven link state routing protocol (OLSR) by providing secure neighbor discovery and authenticated link state updates [6]. SLSP uses digital signatures and assumes that nodes enter the network with asymmetric key pairs and a key management scheme is present to certify the keys in the network.

ODSBR [7] is based on the on-demand DSR routing protocol. ODSBR authenticates its routing packets with digital signatures

and a public key infrastructure is assumed to manage the keys. ODSBR employs a reputation based mechanism to monitor data packets and maintain a path specific rating list. Shared keys are assumed to allow for authenticated acknowledgement messages to be transmitted between a source and probe nodes which provide the evidence for path rating. CONFIDANT [8] is another reputation based solution which does not use any cryptographic techniques and therefore does not require a key management system. CONFIDANT does assume pre-exiting relationships between a small number of nodes called friends. The CONFIDANT is an on-demand solution which provides a node specific reputation list to help selecting secure paths during route discovery.

The observation is made that most secure ad hoc routing protocols assume the existence of a key management system to certify, authenticate, and distribute keying information. Pure mobile ad hoc networks cannot assume the existence of a trusted third party (TTP) and must address the problem of key management.

2. OUR APPROACH

a. System Model

We view the trust problem in ad hoc networks as a weighted trust graph *G(V,E)* where the vertex *V* represent nodes and the edges *E* represent paths. There is no TTP present during communication. The routing environment is on-demand. Each node is assumed to have an asymmetric key pair before entering the network.

We design a key management system to provide key management for secure on-demand routing protocols. The system operation is as follows. A key distribution scheme is proposed which is divided into two components: localized key exchanges and remote end-to-end key exchanges. A local authentication is performed by exchanging keys between close proximity neighbours over a location-limited channel. Remote end-to-end key exchange uses the established localized relationships to share keys remotely across multiple hops. The security evidence provided by certificates is allowed to influence the selection of routes during the route discovery phase. We propose a security evaluation metric which aggregates trust along a path based on a security metric and path distance.

Similar to [14], we consider a fully distributed network of wireless nodes with generic medium access control (such as IEEE 802.11) and secure on- demand routing mechanisms. Nodes can be stationary or move with low to high mobility speeds (0*m/s* -20*m/s*). We assume that there are no pre-existing infrastructure and no form of *online* trusted authority to assist the key distribution mechanism. Since we are considering *authority-based* MANETs as defined in [14], there exists an *offline* authority to bootstrap the system; before users join the network they have to acquire a certificate from the *offline* trusted authority. The trusted authority thus only provides each node with its own certificate and not with the certificates of any other nodes. This requirement is fundamental to ensuring scalability and on-demand network formation. Each node is also issued with the authentic public key of the trusted authority and a universal set of system parameters. The certificate must contain the offline authority's identity, the node's public key and identity/network address, a unique sequence number, certificate generation date and expiry date

b. Key distribution scheme

1) Localized key exchange: Neighbouring nodes can securely exchange keying material without the presence of a TTP. Nodes in close proximity first exchange pre-authentication information across a location-limited channel. Location-limited channels include infrared, physical contact, audio, etc. Because of the nature and characteristics of a location-limited channel like infrared the neighbors can be assured that the pre- authentication is legitimately from the sender. After users exchange pre-authentication information a group certificate exchange scheme is implemented over the main wireless channel. Certificates binding a node's unique ID and public key are exchanged and authenticated using the previously acquired pre- authenticated information.

Following the routing protocol the localized key exchange has two approaches. Firstly following a route request immediate nodes perform a localized key exchange. Alternatively localized key exchange would follow a hello packet broadcast of an on-demand routing protocol like AODV.

2) Remote end-to-end key exchange: The certificate of the source node *A* is forwarded along the request route packet *RREQ* independent of the routing packets. At each hop the intermediate node is inquired if it possesses the source's certificate. If not a separate unicast message is sent back to the previous hop requesting the sources certificate. This procedure follows the *RREQ* until it reaches its target. The destination node *B* caches the sources certificate and replies with a route reply message *RREP*. The *RREP* is forwarded along the reverse path and at each intermediate node the local certificate repository is checked if it contains the destination's certificate. If the certificate is not found a unicast certificate exchange similar to the forward path one is performed. All the certificates are verified on the *REPP* route. This approach minimizes unnecessary certificate verifications on paths which will not be selected.

When a node (RN) receives a routing control packet it checks in its certificate database if it has the certificates of the packet originator (ON) and the previous hop node (PN) on the forward route. If RN has both the certificates of ON and PN (*CertON* and *CertPN*), it can process the control packet as normal. If not, it requests both the certificates from PN. If RN does not have the certificate of PN, then it also sends its own certificate with the request to the previous- hop.

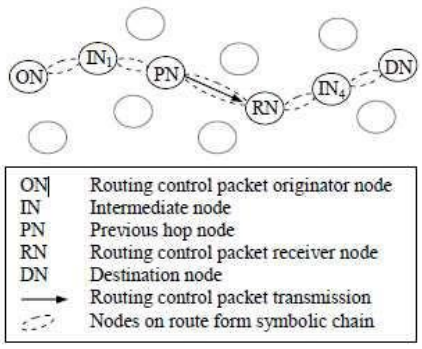

Figure 1: Certificate distribution main procedure

Note that if RN is the first-hop on the route, then the previous-hop node and the control packet originator node will be the same entity. The routing messages thus effectively chain nodes together and allow them to relay all keying material, as required, along the virtual chains.

The proposed key distribution scheme, works as follows:

– When any node in the network receives a RCP it first determines if the originator of the message (ON) has the same network address as the previous hop node (PN) on the forward route, that is, RN has to determine if ON is the first-hop.

In case when the addresses of ON and PN are the same, the RN runs:

Protocol 1:
RN searches its certificate repository for ON certificate

If found,
    Process the routing message RCP
else
    ON and RN Exchange Certificate (Peer-to- Peer)
        $CertRN \rightarrow ON,\ ON \rightarrow CertON$
    Process the routing message RCP

– If the ON address and the previous-hop node (PN) address are not equal, RN runes protocol 2. The RN will search its certificate repository for *CertON and CertPN*.

Protocol 2:
RN searches its repository for CertPN
If Found,
    Search for CertON
        If Found
            No action, process routing packet as normal
        else
            Peer-to-Peer certificate exchange
                $CertRN \rightarrow PN,\ CertPN \rightarrow RN$
else
    Search for CertON
        If Found
            $Cert \rightarrow PN, Cert_{PN} \leftrightarrow RN$
        else
            Peer-to-Peer certificate exchange
                $CertRN \ // \ Cert \rightarrow PN$
                $CertPN \ // \ CertON \rightarrow RN$
            Process routing packet as normal

c. Security Evaluation Scheme

The key distribution scheme follows the route discovery phase exchanging keys locally and remotely. The security evaluation scheme enhanced the route discovery phase. This component's core approach is to provide trust path selection based on both distance and a security metric. The ad hoc network is modeled as a weighted trust graph *G(V,E)* where the edges *E* are nodes with a weighted trust metric *t*. This trust metric is assumed to be available based on either public key certificates or a reputation-based monitoring system. The vertexes *V* represent the weighted paths or routes in the network. We propose an evaluation metric for these weighted paths. We propose the use of the semiring mathematical operators $\oplus$ and $\otimes$ to aggregation trust along a multi-hop path of the ad hoc on-demand protocol. The distance semiring approach uses the operator to aggregate metrics along a path like parallel resistors would be summed ie. $\frac{1}{R_T} = \frac{1}{R_1} + \frac{1}{R_2} + ... + \frac{1}{R_n}$. The aggregated value will decrease along a path and the total is always less than the summations smallest component. This description aligns with our design specifications. The aggregated value will be low for routes with high hop counts. Secondly it will reflect the trust characteristics of a trust chain which states that a chain is only as strong as its weakest link.

Following the route discovery phase, at each hop of a *RREQ* the current path weight is calculated and compared to an implicit path revocation threshold. If the aggregated trust is more than the threshold value the path and associated weight are stored in the routing table corresponding to the reverse route and the *RREQ* is forwarded. Similarly at each hop of a *RREP* the current path weight is calculated and stored in the routing table matching the forward route. Multiple replies to a single *RREQ* are filtered by the hop count metric in standard AODV and DSR on- demand routing protocols. We propose that routes are filtered based on their sequence number and their semiring based weighted path metric. This filters the most recent routes and based on the nature of the weighted path metric, hop count and trust are both accounted for.

3. RELATED WORK

Key management solutions are presented in [9-11]. The self issuing certificate chain approach in [12] proposes a self organized key management solution that treats the network as a weighted direct graph. This proposal is a proactive methods designed for application layer security.

Proximity based key agreement is investigated in [13] and again by Capkun in [14] where security relies upon nodes' mobility to provide multiple close proximity key exchanges. This proposal is limited by its reliance on mobility.

A proactive reputation-based solution is proposed in [15] which operates on the application layer. Semi- ring mathematics [16] is used to realize the proactive generic-single-source-shortest-distance algorithm. The majority of literature mentioned functions in a proactive manner for application layer solutions. We propose a reactive approach for the network layer

4. EVALUATION

Our approach is simulated as a C++ network layer application in ns-2. It is planned for ad hoc on- demand routing protocols and designed on the AODV routing protocol but our solution is not protocol specific. The key distribution scheme is simulated and test in large node environment with varying mobility and load. The packet delivery ratio is examined to investigate how the security mechanism affects the success of the routing protocol. The normalised routing load is investigated to show the overhead of the key exchange components. The security evaluation scheme is difficult to evaluate using simulations. The scenarios is established where the assumed weighted node edges carry a security metric

which identifies fault detection or data transmission errors carried out by nodes for example in [7, 8]. This allows the proposal to protect against black hole attacks. Simulations are set up which investigate the packet delivery ratio with a changing number of adversary nodes.

i) Performance Metric

The following quantitative metrics are used to analyze the performance of the routing protocols in mobile ad hoc networks.

(a) Packet Delivery Ratio: The packet delivery ratio (PDR) represents the percentage of data packets that are successfully received by their intended destination. This metric is also known as throughput and is considered a measurement of the effectiveness of a routing protocol. The equation for PDR is:

$$PDR\% = \frac{\sum_1^n CBRrec}{\sum_1^n CBRsent} \times 100$$

where $\sum_1^n CBRrec$ and $\sum_1^n CBRrec$ are the number of CBR data packets received and sent respectively.

(b) Routing Overhead: A routing protocol uses control packets to establish routes on which data packets are transmitted. Control packets are separate from data packets but share the same communication channel. Due to the lack of channel capacity in mobile ad hoc networks a large number of control packets can result in poor network performance. Key management would require additional control packets to achieve key management functionality this will be reflected in the simulations. The routing overhead is also known as a routing protocol's internal efficiency and will represent the number of control packets used for a given protocol.

(c) Average End-to-End Delay: This is a qualitative measurement of the delay of data packets. The average end-to-end delay of a data packet is the time from which it is created at the source and when it arrives at the intended destination. The delay includes propagation and queuing delay. Delay can be caused by a high number of control packets propagating in the network or a high computational overhead for the given protocol. The average end-to-end delay is calculated as follows,

$$End\ to\ End\ Delay = \frac{\sum_1^n (CBRsendtime - CBRrecvtime)}{\sum_1^n CBRrec}$$

where *CBRsendtime* and *CBRrecvtime* represent the record times that a CBR data packet was sent and received

ii) Simulation Model

A routing protocol was designed in C++ based on the AODV routing protocol available in the ns-2.31 package. The routing protocol is programmed as a routing agent class. The routing agent handles the establishment of routes and certificate distribution. Modifications are made to the AODV routing agent at the *RecvRequest*, *SendRequest*, *RecvReply*, and *SendReply* functions. These modifications allow for the distribution of separate certificate packets, triggered by the routing packets. The routing agent's packet header was modified to include a certificate control packet *CertS*. The size of the certificate included is 450 bytes. The size of the certificate control packets is increased resulting in an effective delay in communication simulating the transfer of actual certificates. A certificate table is included at each node *CertTable* which is updated by certificate control packets. The certificate table is linked to the routing table and each node is responsible for managing its own certificate table.

A simulation *tcl* file is written to setup the mobile ad hoc network's desired simulation scenario, traffic and mobility model. The trace support files in ns-2.31 were modified to support the routing agent allowing the inclusion of certificate control packets and trust information. As a result the output trace and *nam* files reflect the operation of the routing agent. Figure 2 shows a sample output of the *nam* simulation file.

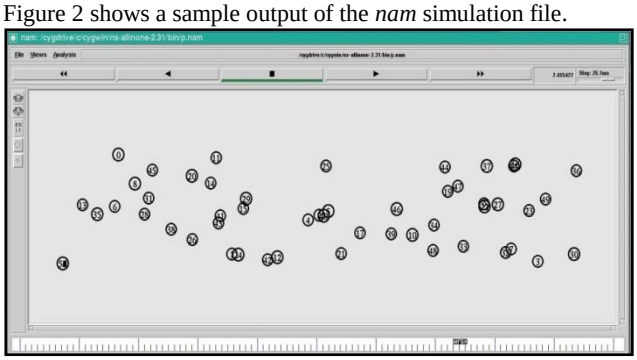

Figure 2: Sample *nam* simulation file illustrating typical network topology

iii) Packet Delivery

The packet delivery results for the AODV routing protocol is presented in Figure 3 & 4. Figure 3 represents a simulation environment with a pause time of 0 seconds. This represents a network of nodes that are continually moving, while Figure 4 represents a partially stable network. The observation is made that as the speed increases both protocols throughput decreases. At high speeds the network topology changes rapidly causing breakages in routing links. The reduction in packet delivery at high speeds is because both protocols will drop data packets as a result of increased routing breakages. The stable network in Figure 4 shows better performance at higher speeds because the number of route link breakages is reduced as a result of a larger pause time. A large pause time represents a network that will move at a given speed then pause in a fixed location for a set amount of time. During this time routing link breakages are not expected until movement commences again.

A certificate distribution scheme would expect a severe reduction in performance due to an excessive number of packets being transmitted in the network or the additional size of the control packet. A conventional certificate distribution scheme, suggested as a possible solution in [8], simply includes the source certificate in the request packets *RREQ* and the destinations certificate in the reply packets *RREP*. This method was implemented as a separate routing agent *AODVcert* in ns2. A similar method is suggested in [6]. Implementation includes increasing the packet size of the routing control packets to include a 450 byte certificate. This effectively increased the regular 56 byte AODV route control packets to 506 bytes. Such an approach would result in the simplest method of certificate distribution but transmitting 450 bytes more data per control packet would severely reduce the network performance.

5. CONCLUSION

It is concluded from investigation of existing secure ad hoc routing protocols that the majority assume the existence of a key

management system to distribute and manage the asymmetric or symmetric keys. We propose a key management solution that provides a key exchange scheme and a security evaluation scheme. The proposal is design for an on-demand ad hoc routing protocol.

Simulations in ns-2 investigate the packet delivery ratio of the solution's key exchange scheme compared at varying load and mobility. The security evaluation scheme allows for the most trusted route to be selected during the route discovery phase. An available security metric is assumed and simulations investigate the success of preventing black hole attacks.

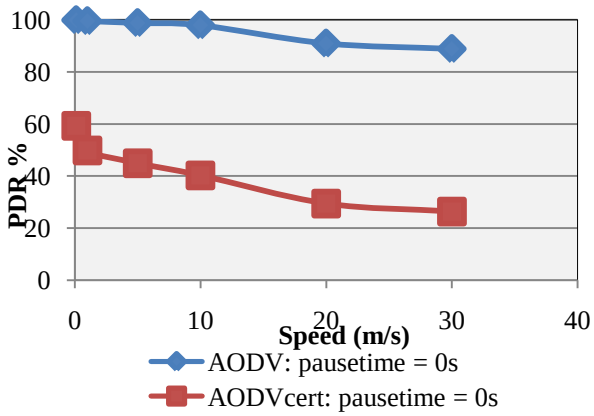

Figure 3: Packet Delivery Ratio for highly mobile network (0 second pause time)

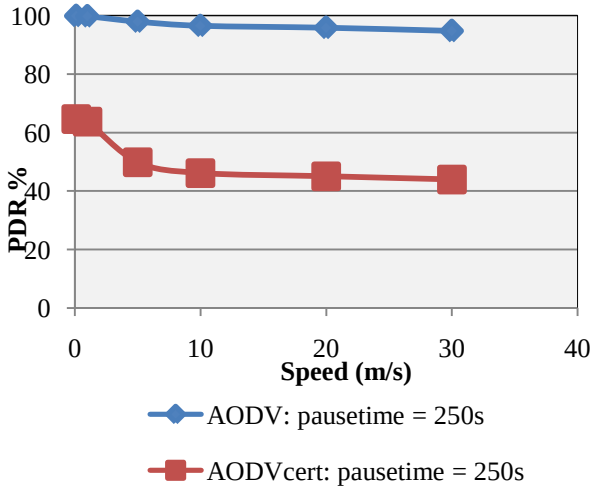

Figure 4: Packet Delivery Ratio for partially stable network (250 second pause time)

5. REFERENCES

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", in ***Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*: IEEE Computer Society**, 2002.

[2] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", ***Wireless Networks***, vol. 11, pp. 21-38, 2005.

[3] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and Secure Source Authentication for Multicast", **Network and Distributed System Security Symposium (NDSS'01)**, 2001.

[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks" in ***Proceedings of the 10th IEEE International Conference on Network Protocols*: IEEE Computer Society**, 2002.

[5] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," ***SIGMOBILE Mob. Comput. Commun. Rev.***, vol. 6, pp. 106-107, 2002.

[6] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in ***Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*: IEEE Computer Society**, 2003.

[7] B. Awerbuch, R. Curtmola, D. Holmer, C.Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," ***ACM Trans. Inf. Syst. Secur.***, vol. 10, pp. 1-35, 2008.

[8] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in ***Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing,*** Lausanne, Switzerland: ACM, 2002.

[9] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenets," in ***Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing,*** Long Beach, CA, USA: ACM,2001.

[10] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," ***IEEE Network: special issue on network security***, vol. 13, pp. 24-30, 1999.

[11] D. B. Smetters, D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "**Talking To Strangers: Authentication in Ad-Hoc Wireless Networks**," 2002.

[12] S. Capkun, L. Butty, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," ***IEEE Transactions on Mobile Computing***, vol. 2, pp. 52-64, 2003.

[13] A. Scannell, A. Varshavsky, A. LaMarca, and E. D. Lara, "Proximity-based authentication of mobile devices," ***International Journal Secure Networks***, vol. 4, pp. 4-16, 2009.

[14] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Mobility Helps Peer-to-Peer Security," ***IEEE Transactions on Mobile Computing***,vol. 5, pp. 43-51, 2006.

[15] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," ***IEEE Journal on Selected Areas in Communications***, vol. 24, pp. 318-328, 2006 2006.

[16] M. Mohri, "Semiring frameworks and algorithms for shortest-distance problems," ***Journal on Autom. Lang. Comb.***, vol. 7, pp. 321-350,2002.