Simulation of the Performance Metrics for Securing DSDV Routing Protocol Based on Trusted Environments

Chiang Ling Feng*
Department of Electric Engineering, ChienKuo Technology University, Taiwan

*Corresponding author email: acclaim0629v@gmail.com

Abstract. To organize the network in an efficient way to minimize the risk of illegal node and to safeguard protected information, a security mechanism is required to secure communication. In addition, a security mechanism is also required to ensure that received information have not been tampered with. In this paper, a more efficient mechanism for Securing the Destination Sequenced Distance Vector Routing Protocol (SDSDV) is proposed. This paper comprehensively investigates the performance impacts by varying the number of maximum connections and mobility on securing the ad hoc network with Destination Sequenced Distance Vector Routing Protocol (DSDV) Routing Protocol. From simulation results, we explore the causes for performance degradation. Based on the investigation, we indicate that we have to impose restrictions on the maximum connections to acquire an expected performance. These results also reveal that the performance decreases with the increment of the mobility and maximum connections that is unequal to 60. If we want to obtain the optimal performance, the number of nodes in a network should be constrained to be 60 if the maximum connections are 60.

Keywords: Mobility, maximum connections, mobile Ad hoc networks, modified SDSDV, hash function.

1. Introduction
Ad hoc network is a network with dynamic topology and may change randomly and rapidly at unpredictable times. Due to the fact of the vulnerability of channels, the possibility of denial-of-service attacks will increase due to the physical security treats in mobile wireless networks. The significant objective of ad hoc networks is to provide robust communication in a variation of environments. When a malicious node hijacks the network bandwidth by generating frequently unnecessary route requests, the network resources will be unavailable to other nodes or non-existent nodes and the network no longer operates correctly or crashes. In mobile Ad hoc networks, the system performance relies on cooperative routing. However, a selfish node [1-5] is defined as whom does only forward the control packets to gain his routing information about the networks, which refuses to forward data packets. But, the issue of selfish nodes is beyond the scope of this work. Hence, DSDV routing protocol is assumed that all nodes are trustworthy and cooperative here.

Since any attacker can simply look at the contents of packet, effectual algorithm and secret keys are two fundamental components in a cryptographic system. Specifically, a secret key should be not apt to be found and decrypted. One of the primary challenges in cryptography is how to implement the cryptography in wireless mobile networks. In general, secret-key algorithm is often used to protect the actual data. To decrypt the public-key encryption algorithm is more difficult due to the characteristic of key pair that one key used by the sender (private key) and one key used by the receiver (public key).
Even if we know the public key of the peer, it is extremely difficult to figure out its private key unless the transaction of key’s negotiation is eavesdropped. However, mobility transparency is an essential requirement in mobile wireless system to provide seamless mobility in any heterogeneous networks. This paper first depicts the design’s considerations and the literature survey is given in section 2. The implementations of security in our proposed MDSDV routing protocol in section 3 to enhance the security property of existing routing protocol. We present the system performance due to mobility and maximum connections in section 4. And the simulation results and detailed discussions are also given. Finally, we draw our conclusions in section 5.

2. Literature Survey
To safeguard protected information and ensure that the received information has not been tamped with, secure efficient distance vector (SEAD) has been proposed in [6-7] based on trusted environments. This proposed protocol can prevent a malicious node from modifying a sequence number or cost metric of an advertised route by using one-way hash function and does not use asymmetric cryptographic operation to guard against denial-of-service attacks. SDSDV [8] protects all messages combining with message authentication using pairwise shared keys. The message authentication code of a message is immediately sent after transmission of the message is finished. Any nodes in SEAD network cannot successfully re-advertise the route with a distance shorter than 2. It also cannot prevent a malicious node from advertising a distance of 2 or longer. SDSDV also incurs a significant network overhead than DSDV because it has to check the consistency of an updated route due to the persistently changes of the sequence number, distance, or the next hop [8]. Based on the balance between the robustness of security and system performance, we are willing to have a similar risk on the security but produce a significant enhancement of the system performance as possible. Since any attacker can simply look at the contents of packet, effectual algorithm and secret keys are two fundamental components in a cryptographic system. Specifically, a secret key should be not apt to be found and decrypted. Mobility transparency is an essential requirement in mobile wireless system to provide seamless mobility in any heterogeneous networks. Therefore, we modify the algorithm of SDSDV routing [8, 9] using the encryption of pairwise shared secret key [10-14] to achieve the optimal performance as possible as that of original DSDV routing protocol.

3. MSDSDV Routing Protocol
In DSDV, each mobile node maintains a completely routing table containing routing information to every node in the network. The routing information includes all available destinations, the metric and next hop to each destination, and a sequence number generated by the destination node. Each node attempts to periodically update the routing table or when significantly available routing information is acquainted to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network. Sequence numbers and metric values containing in each update play a vital role in DSDV operation. However, a malicious node can easily disrupt the routing protocol by arbitrarily tempering the sequence numbers or the metrics. To enhance the robustness of DSDV routing protocol, we will review the security mechanism of SDSDV and characterize our MSDSDV (modified SDSDV) security mechanism in this section.
To provide a more realistic application in mobile wireless ad hoc network is not an easy task. SDSDV [8, 9] based on the regular DSDV protocol is particularly designed for wireless Ad hoc network. In order to establish a multi-hop route, SDSDV provide the voluminous information. Due to this reason, a hijacker can analyze the network topology to perform the attack of service of deny focusing on some critical nodes. Therefore, we modify the concept of SDSDV and implement it on the practical wireless mobile Ad hoc system based on the realistic security roaming. The major goal of our proposed SDSDV, denoted as MSDDSDV, is to protect the sequence numbers and metrics in each entry of an update from being arbitrarily changed. To achieve this goal, hash chain is implemented to prevent the attack from arbitrarily tampered. We also adopt an authentication tag in the transmitted route to verify the integrity and authenticity of transmitted information. Authentication tag is a function of the node’s identification (such as sequence number and cost metric) and the pairwise shared secret key. Authentication tag is
computed by the simple hash function. Let $V$ be a set of nodes. For $v_i, v_j \in V$, assume $r_{v_i \rightarrow v_j}$ to be the route from node $v_i$ to node $v_j$. Denotes $\text{seq}(v_i, v_j)$ and $\text{cst}(v_i, v_j)$ are the current sequence number and metric of $r_{v_i \rightarrow v_j}$, respectively. For $\forall v_i \in V$, $v_i$ constructs a hash chain, denoted as $h'(x_i)$, from a secret $x_i$.

Therefore, we can replace the notation $h'(x_i)$ in SDSDV routing protocol by the notation $\left[\left[\left[\left[|,|,\ldots,,\ldots,\right],\ldots,\ldots,\right],\ldots,\ldots,\right],\ldots,\ldots,\right]$ in our proposed security scheme. Where the notation $\left[\left[\left[\left[|,\ldots,\ldots,\right],\ldots,\ldots,\right],\ldots,\ldots,\right],\ldots,\ldots,\right]$ denotes that a plaintext $X$ is encrypted by the pairwise shared secret key $K_{i,j}$ which node $v_i$ shares with node $v_j \in V$, $i \neq j$. The symbol $|$ represents concatenation of the information. But, instead of the statement in SDSDV routing protocol, $K_{i,j}$ is transmitted only at the phases of routing discovery and updated route, and is not sent combining with the message to node $v_j$ to avoid the same-distance fraud attack to prevent the attack from arbitrarily tampered.

We assume some mechanisms are available for a node to deploy the authentication protocols and the authentic elements from its generated hash chains. Let the notation $D_{K_{i,j}}[X]$ represent the decrypting procedure of received message $X$ using $K_{i,j}$. Therefore, when a neighbour node receives the forwarded packet,

$$r_{v_i \rightarrow v_j}\left(\text{seq}, \text{cst} + 1\right) = D_{K_{i,j}}[E_{K_{i,j}}[r_{v_i \rightarrow v_j} \left| h'(\text{seq}(v_i, v_j)), \text{cst}(v_i, v_j)\right]]$$

Equation (1) is used to authenticate the adjacent node by computing the received sequence number and metric, which are received from the neighbour. Since security algorithm is designed for the protection of the network infrastructure, the packet is discarded and no action is executed if the constrained condition is mismatched. Otherwise, the receiving node encrypts its own routing table with the pairwise shared secret key related to the next hop if one of the following conditions is satisfied.

1. $\text{seq} > \text{seq}'$
2. $\text{seq} = \text{seq}'$ and $\text{cst} < \text{cst}'$

4. Simulation and Environment and Parameters

To comprehensively measure the performances among DSDV, SDSDV, and MSDSDV, the impact of the performance metrics must be evaluated. When a node is out of the communication range with the neighbour, a transmitted packet will be dropped. Therefore, the packet delivery fraction which is defined as the fraction of the data packets, generated by the source node, that are successfully delivered to the final destination node along the discovered routes can be used to evaluate the ability of the protocol to discover routes and to reflect the maximum throughput that the network can support.

The simulation was done with ns2 simulator [15]. First, we assume that no means can be used to obtain the spatial information of nodes with respect to other nodes in this network. Each node is initially placed at a random location and moves according to the random waypoint mobility model. The moving speed ranges from 5 and 25 m/s. The destination node in the simulation environment is randomly chosen by each node at the beginning of the simulation. When a node reaches pre-selected location, we assume that this node stays for a period of time (assumed to be zero here), and then chooses a new location at random and moves with a randomly and uniformly chosen velocity. This process of pausing and selecting a new destination to which to move is repeated.

In order to address mobile limitations in IEEE 802.11 network, the physical channel bit rate is set to 2 Mbps CBR traffic for IEEE 802.11 DCF and the nominal radio range is 250 m communication range to satisfy the requirement of this standard. The size of application data payload size is 512 bytes for each packet. The number of active stations, denoted as $nn$, which have some data to be sent, in our simulated scenario is varied from 30 to 90. The number of maximum connections, denoted as $mc$, in our simulated scenario is varied from 20 to 80. For the routing zone radius for our simulation, the nodes are assumed to be uniformly distributed in 600 m * 600 m two-dimensional square spaces. The simulation time is selected to be 1000 seconds to stabilize the simulation results. All the mobile nodes are assumed to be in the communication range and move with the same constant speed.
Maximum connections, packet delivery fraction, mobility, and mean delay metrics are used to evaluate the security protocol. We change the only one parameter and maintain the others unchanged to clarify the effect of changed parameter as much as possible for each comparison. Altering the value of $mc$ makes the first comparison. Each connection is specified as a randomly selected source-destination pair. Figure 1 and figure 2 show the packet delivery ratio versus maximum connections with respect to the DSDV, SDSDV, and MDSDV routing protocol for number of nodes being 30 and 40, respectively. From all of these figures, we see that packet delivery fraction gets worse when $mc$ increases. The packet delivery fraction does not have much impact on the performance between DSDV routing protocol and DSDV routing protocol. But, MDSDV has better performance than SDSDV. We also see that increasing the number of active stations will decrease the packet delivery fraction. It means that the ratio of dropped packets increases. However, the position at $mc=60$ seems to be worthy of discussion. Increasing the value of $mc$ for each node, it represents that each node nearly has more direct links to all others in the network. Two or more transmitted packets to a same link are considered as collided packets at the same time. Therefore, the packet delivery ratio decreases because the probability of colliding packets increases.

To ensure the correction of our inference for the distinctive characteristic of $mc$ related to each routing protocol in advance, we illustrate simulation result with the example of MDSDV. Varying the value of $nn$ makes second comparison. In a mobile network, we allow mobile node to roam within the specific network. Therefore, the moving speed of nodes and the number of connections should be considered to evaluate the performance of MDSDV routing protocol and compare it with DSDV and SDSDV routing protocol. From figure 3, we can infer no obvious change in the throughput performance among DSDV, SDSDV, and MDSDV routing protocols for each moving speed. However, under the same traffic loads, we see that the increment of mobility of nodes will create the amount of update of the network topology and result in the degradation in network performance.

![Figure 1](image1.png)

**Figure 1.** The packet delivery ratio versus maximum connections ($mc$) at $nn=30$.

![Figure 2](image2.png)

**Figure 2.** The packet delivery ratio versus maximum connections at $nn=40$.

We also examined the dependence of the delay on each routing protocol at various maximum connections and mobility. We plot the results of average delay of a packet incurred by these three securing routing protocols at speed=5 m/sec and speed=20 m/s based on $mc = 20$, respectively. From figure 4, we see that MDSDV routing protocol offers lower average delay time than SDSDV. The higher
system’s processing loads incurred because every node spends extra time to achieve encryption and decryption mechanism. An extra delay of route maintenance incurred when the mobility increases. These protocols suffer from higher average delay time resulting from both higher probabilities to repair the broken links and the time to report link failure if these broken links cannot be repaired.

![Figure 3. The performance impact of mobility.](image)

When a node moves in or out of range with respect to each other, nodes first try to communicate with other nodes to maintain the connectivity information related to a changing topology. If possible connections are not found, the host will attempt to discovery a new connection for the destination. In this section, we plot the routing overhead incurred by these three securing routing protocols at speed=5m/sec and speed=20 m/s based on $mc=20$, respectively. Figure 5 illustrates that the mobility seems to be not affected by the routing overhead at same moving speed (mobility) among these three routing protocols. This reason is that periodic updates are executed. However, the performance of MDSDV is better than that of SDSDV. In addition, when the mobility increases, unnecessary route reconstructions (i.e., to discover and maintain the communication paths) can be caused from frequently periodic and triggered updates.

![Figure 4. The impact of mobility on the delay performance.](image)

5. Conclusions
In this paper, the vulnerabilities of DSDV and SDSDV routing protocols have been extensively studied. The solution has been carried out based on our proposed MDSD routing protocol in order to prevent attacks. Our proposed routing protocol does not require any additional security functionality to obtain enhanced performance. Our analysis results indicate that the performance is obviously decayed in network if the number of maximum connections is more required. However, the packet delivery fraction is independent of the use of DSDV, SDSDV, and MDSDV routing protocols at a fixed mobility. Suitable parameter selection obviously enhances the performance in the network. For the mobility, we observe that the packet delivery fraction significantly varies at the environments with mobility and nodes. In addition, reducing the number of maximum connections obviously enhanced the system performance in a network.
Figure 5. The impact of mobility on the routing overhead.

References

[1] K. Paul and D. Westhoff, “Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks”, Proc. of IEEE GLOBECOM, Taiwan, China, November, 2002

[2] L. Anderegg and S. Eidenbenz, “Ad hoc-VCG: A Trustful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents”, Proc. of ACM MobiCom, San Diego, September, 2003

[3] S. Zhong, J. Chen, and Y.R. Yang, “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks”, Proc. of IEEE Infocom. San Francisco, April 2003

[4] Yanchao Zhang, Wenjing Lou, and Yuguang Fang, “SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks”, WCNC 2004, pp. 1679-1684, 2004

[5] Jyu-Wei Wang, and Yi-Ping Lin, “A Secure DSDV Routing for Ad hoc Mobile Networks”, Mobile Computing Workshop 2004, pp. 413-418, 2004

[6] L. Buttyan and J.P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” ACM Journal for Mobile Networks (MONET), Vol. 8, No. 5, October 2003

[7] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks”, Ad hoc Networks, Vol. 1, pp. 175-192, 2003.

[8] Tao Wan, E. Kranakis, and P.C. Van Oorschot, “Securing the Destination Sequenced Distance Vector Routing Protocol”, The Proceedings of the 6th International Conference on Information and Communications Security. LNCS, Vol. 3269, pp. 358-374, October, 2004

[9] J. Cardinal, G. Van Assche, “Construction of a shared secret key using continuous variables”, Proceedings. 2003 IEEE Information Theory Workshop. pp.135-138, March-April 2003

[10] B. Preneel, R. Govaerts, and J. Vandewalle, “Hash functions for information authentication”, Proceedings in Computer Systems and Software Engineering, pp. 475 – 480, May 1992

[11] Xun Yi and Kwok Yan Lam, “Hash function based on block cipher”, Electronics Letters, Vol. 33, Issue 23, pp. 1938-1940, November 1997

[12] G. Tsudik, “Message authentication with one-way hash functions”, INFOCOM ’92, Vol. 3, pp. 2055 – 2059, May 1992

[13] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, “The KryptoKnight family of light-weight protocols for authentication and key distribution”, IEEE/ACM Transactions on Networking, Volume 3, Issue 1, pp. 31 – 41, February 1995.

[14] U.M. Maurer, “Secret key agreement by public discussion from common information”, IEEE Transactions on Information Theory, Vol. 39, Issue 3, pp. 733-742, May 1993.

[15] Kevin Fall and Kannan Varadhan, The ns Manual (formerly ns Notes and Documentation). The VINT Project, 2001.