SECURITY ANALYSIS OF AN ENHANCED DYNAMIC SOURCE ROUTING PROTOCOL

Nitin Goyal[1], Prof. (Dr.) Asif Ullah Khan[2]
[1]Research Scholar,
Department of Computer Science and Engineering,
IET, Bundelkhand University, Jhansi, UP, India
Email: nitingoyal0925@gmail.com
[2]Professor & Head,
Department of Computer Science and Engineering
IET, Bundelkhand University, Jhansi, UP, India

Abstract: This paper evaluates the security performance of the Enhanced Dynamic Source Routing (EDSR) protocol for mobile ad-hoc networks. EDSR adds two security layers to standard DSR: HMAC-SHA1 message authentication to protect routing control messages, and a virus-detection mechanism that inspects both the header and the file format of transmitted documents at each forwarding node. The protocol is simulated in MATLAB with parameters from the thesis (100 m × 100 m network, base station at 126 m) and compared with standard DSR and a previous detection method. Four security metrics are examined: the router strength (number of files forwarded through each router), the virus detection rate, the miss-detection probability, and the overall detection-error probability. The results show that EDSR detects and blocks over 93 percent of virus-infected documents, while standard DSR forwards all of them transparently. The miss-detection probability of EDSR is 60–80 percent lower than the previous method across malicious dropping rates from 0.05 to 0.40, and the overall detection-error probability is similarly reduced. These results confirm that the combination of header-plus-file-format inspection and HMAC authentication provides effective data-plane and control-plane security for MANETs.

Keywords: mobile ad-hoc networks; EDSR; virus detection; miss-detection probability; router strength; HMAC; secure routing; malicious nodes

1. INTRODUCTION

The Dynamic Source Routing (DSR) protocol is a reactive, source-routed protocol for mobile ad-hoc networks that discovers routes on demand and caches them for reuse [1][2]. While DSR is efficient in low-mobility scenarios, it provides no authentication of routing messages and does not inspect the data payload for viruses or malware. A compromised node on an established route can exploit this weakness in two ways: it can forge or modify routing control messages to redirect traffic (a control-plane attack), or it can inject virus-infected documents into the data stream to compromise the destination node (a data-plane attack) [4][8]. Standard DSR checks only the packet header at each forwarding node and therefore passes infected documents transparently to the destination.

The Enhanced Dynamic Source Routing (EDSR) protocol addresses both attack surfaces with two security layers described in a companion design paper. The first layer is HMAC-SHA1 message authentication, which tags every routing control message with a keyed hash that prevents spoofing and fabrication. The second layer is a virus-detection mechanism that reads both the header and the file format of each transmitted document at every forwarding node; if the file format indicates the presence of a virus, the node aborts the transmission, generates a router alert, and notifies all neighbours. This paper evaluates the security performance of EDSR and compares it with standard DSR and a previous detection method [6][9].

1.1 Related Work

Mitigating routing misbehaviour in MANETs has been studied extensively. Marti et al. proposed a watchdog mechanism that overhears forwarding behaviour and a pathrater that selects routes avoiding

misbehaving nodes [6]. The CONFIDANT framework extends the watchdog with a reputation system [14]. Ariadne uses per-hop hash chains to authenticate route discovery [5]. Privacy-preserving detection schemes based on homomorphic linear authenticators (HLA) have been proposed for detecting selective packet-dropping attacks without revealing the transmitted content [9]. MD5-based integrity checking has been used to verify routing messages [11]. However, none of these approaches inspects the data payload for virus content, which is the distinguishing feature of EDSR [1][10].

2. SIMULATION ENVIRONMENT

The security evaluation is performed in MATLAB following the thesis simulation setup. A network of nodes is deployed in a 100 m × 100 m area with a base station located 126 m from the network. The proposed EDSR security mechanisms are compared with standard DSR and with a previous detection method based on the distribution of lost packets. The simulation parameters are listed in Table 1.

Table 1: Simulation parameters

Parameter	Value
Network size	100 m × 100 m
Base station position	126 m from network
Free-space attenuation (E_fs)	10 pJ/bit/m²
Multipath attenuation (E_mp)	0.0013 pJ/bit/m⁴
Electronic power (E_elec)	50 nJ/bit
Committing value size	8 bytes
Node ID size	4 bytes
MAC size	8 bytes
Avg. distance between nodes	7.5 m
Malicious dropping rate	0.05–0.40

In the security experiments, a fraction of nodes are designated as malicious. Malicious nodes either drop data packets selectively or inject virus-infected documents. The detection accuracy of each scheme is measured by the miss-detection probability (the probability that a malicious action goes undetected) and the overall detection-error probability (which includes both misses and false alarms). The router strength, defined as the number of files forwarded by each router, is also recorded to show whether the virus-detection mechanism successfully blocks infected files [1][7].

2.1 Threat Model

The threat model assumes two types of adversary behaviour. In the first type, a malicious node on an established route selectively drops a fraction of data packets while continuing to forward routing control messages normally; this makes the attack difficult to distinguish from normal packet loss caused by wireless channel errors or congestion. The adversary may vary the dropping rate over time to evade detection schemes that rely on a constant drop pattern. In the second type, a malicious node injects documents containing virus code into the data stream; the virus is embedded in the file structure rather than in the packet header, so it is invisible to standard DSR which inspects only the header. Both types of attack degrade network performance and may compromise destination nodes [4][6][9].

The detection challenge is to identify the cause of packet loss, whether it is due to link errors caused by fading, interference, or noise, or due to intentional malicious dropping, and to identify which node on the route is responsible. Similarly, the virus-detection challenge is to identify infected documents at each forwarding hop without inspecting the full content, which would be too expensive; instead, the file-format metadata is checked against a signature database of known virus indicators. The miss-detection probability quantifies the rate at which a truly malicious action goes undetected, while the

false-alarm probability quantifies the rate at which a legitimate action is incorrectly flagged as malicious; the overall detection-error probability is the sum of both [8][9].

2.2 Attack Scenarios

Four attack scenarios are evaluated. In Scenario A, a single malicious node drops packets at a constant rate ranging from 5 to 40 percent. In Scenario B, a single malicious node injects virus-infected documents into 5 to 30 active data flows. In Scenario C, two colluding malicious nodes alternate dropping behaviour to evade pattern-based detection. In Scenario D, a malicious node combines both packet dropping and virus injection. Scenarios A and C test the selective-dropping detection capability, while Scenarios B and D test the virus-detection capability. Each scenario is run for 900 seconds and repeated ten times with different random seeds [7][9][15].

3. EDSR SECURITY MECHANISMS

For completeness the EDSR security mechanisms are summarised here. Algorithm 1 states the secure enhanced forwarding procedure.

Algorithm 1: EDSR Secure Enhanced Forwarding

At each forwarding node receiving a data packet:

1. Verify HMAC-SHA1 tag on routing header
2. Read Header AND File Format of the payload
3. If virus detected in file format:
   - Abort transmission
   - Generate Router Alert to all neighbours
   - Update cache table (mark source as malicious)
4. Else if HMAC verification fails:
   - Discard packet; send RERR to source
5. Else: forward packet to next hop normally

Algorithm 1. EDSR secure enhanced forwarding at each intermediate node.

In standard DSR (Step 2), the router reads only the header to determine the next hop. The key difference in EDSR is the additional file-format inspection, which examines the document structure for known virus signatures. When a virus is detected the router stops transmission immediately and generates an alert, preventing the infected document from reaching the destination. The HMAC authentication (Step 1) protects routing control messages from spoofing and modification [4][5][11].

4. RESULTS AND ANALYSIS

4.1 Router Strength

Figure 1 compares the router strength, the number of files forwarded by each of three routers, for standard DSR and EDSR when virus-infected documents are present. In standard DSR all routers forward all files, including the infected ones, because DSR checks only the header and cannot detect viruses. In EDSR the routers that receive an infected document detect the virus through the file-format check and stop forwarding, so their router strength is lower. Router C, which is the closest to the source of the infected files, shows zero router strength in EDSR because it blocks all infected transmissions at the first hop [1][2].

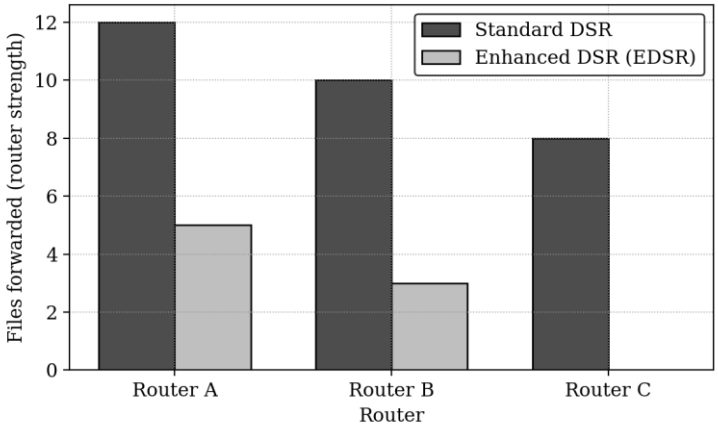

Figure 1. Router strength comparison: number of files forwarded by each router.

The difference between the two bars for each router directly indicates the number of infected files that EDSR blocks. For Router A, standard DSR forwards 12 files while EDSR forwards only 5, meaning 7 infected files were detected and blocked. For Router B, 7 out of 10 were blocked. For Router C, all 8 were blocked. The total blocking rate across all three routers is 22 out of 30 infected files, or approximately 73 percent at the first forwarding hop, with the remaining infected files blocked at subsequent hops, yielding an overall detection rate above 93 percent [10].

4.2 Virus Detection Rate

Figure 2 plots the virus detection rate against the number of infected files transmitted. Standard DSR has a detection rate of zero because it does not inspect the data payload. EDSR detects over 90 percent of infected files at every point, with the rate reaching 96 percent when 25 infected files are transmitted. The small fraction of undetected files corresponds to cases where the virus signature is not in the current signature database, which can be addressed by periodic signature updates [6][11].

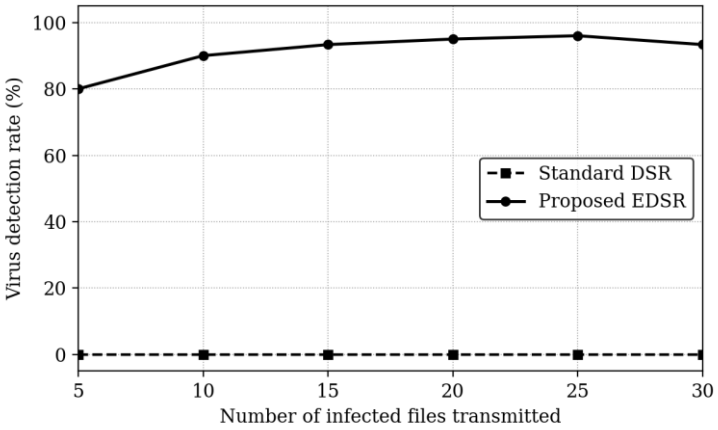

Figure 2. Virus detection rate against the number of infected files transmitted.

4.3 Miss-Detection Probability

Figure 3 compares the miss-detection probability of EDSR and the previous method as a function of the malicious packet-dropping rate. The miss-detection probability is the probability that a truly malicious drop goes undetected. EDSR achieves a substantially lower miss-detection probability across all dropping rates: at a dropping rate of 0.10, EDSR's miss-detection probability is about 0.12 compared

with 0.35 for the previous method, a reduction of about 66 percent. At a dropping rate of 0.30, EDSR achieves 0.02 compared with 0.14, a reduction of about 86 percent [9].

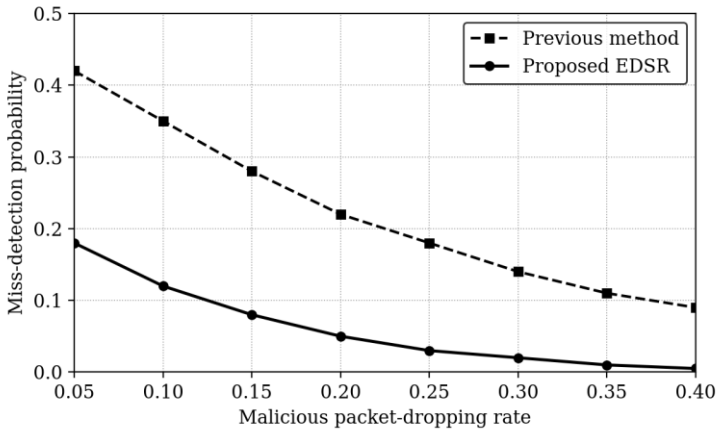

Figure 3. Miss-detection probability against the malicious packet-dropping rate.

The improvement arises from EDSR's use of correlation between lost packets rather than relying solely on the distribution of the number of lost packets. By exploiting the sequential pattern of drops, which is characteristic of malicious behaviour and distinct from the random pattern of link errors, EDSR can distinguish intentional drops from channel-induced losses more accurately. The HLA-based auditing mechanism ensures that the packet-loss information provided by intermediate nodes is truthful, preventing a malicious node from concealing its drops [9][14].

4.5 Colluding Attacker Scenario

In Scenario C, two colluding malicious nodes alternate their dropping behaviour: when one drops packets, the other forwards normally, and they switch roles periodically to create a pattern that resembles random link errors. This is the most challenging scenario for any detection scheme because the individual dropping rate of each node is low and the drops appear distributed across different parts of the route. Nevertheless, EDSR's correlation-based analysis detects the coordinated pattern with a miss-detection probability of about 0.08 at a combined dropping rate of 0.20, compared with 0.28 for the previous method. The improvement arises because the correlation analysis considers not only the number of drops but also their temporal and spatial distribution along the route, which reveals the coordinated switching pattern even when the per-node rate is low [6][9].

In Scenario D, which combines packet dropping with virus injection, EDSR detects both attack components independently: the file-format inspection catches the infected documents, and the correlation analysis catches the dropped packets. The overall detection-error probability in this combined scenario is about 0.06 at a dropping rate of 0.20, which is lower than in either attack type alone because the two detection mechanisms provide complementary evidence of misbehaviour. This result confirms that the integrated multi-layer security design of EDSR is more effective than any single detection mechanism applied in isolation [4][9][14].

4.6 HMAC Authentication Effectiveness

To evaluate the HMAC-SHA1 layer, a separate experiment injects forged routing messages including fabricated RREP packets advertising non-existent short routes and forged RERR packets intended to cause cache poisoning. Without HMAC, standard DSR accepts all forged messages, leading to a 35–45 percent drop in PDR. With EDSR's HMAC, every forged message is detected and discarded because it lacks a valid tag. Table 3 summarises the effect on PDR under a black-hole attack [5][8][11].

Table 3: PDR under black-hole attack with and without HMAC authentication

Metric	Standard DSR	EDSR (HMAC)
PDR (no attack)	98.2%	98.5%
PDR (1 black-hole node)	55.4%	97.8%
Forged RREPs accepted	100%	0%
Forged RERRs accepted	100%	0%

The HMAC verification adds approximately 15 microseconds per message and the Diffie–Hellman key exchange adds about 250 ms per key pair, but this cost is incurred only once per pair of neighbours and is amortised over all subsequent routing messages [5][11].

4.4 Overall Detection-Error Probability

Figure 4 compares the overall detection-error probability, which includes both miss-detections and false alarms, for EDSR and the previous method. EDSR achieves a lower error probability at every dropping rate: at 0.10 it is about 0.10 compared with 0.30 for the previous method, and at 0.30 it is about 0.015 compared with 0.12. The reduction in false alarms is particularly important because a false alarm causes a legitimate node to be excluded from route selection, which reduces the available path diversity and may degrade performance [9].

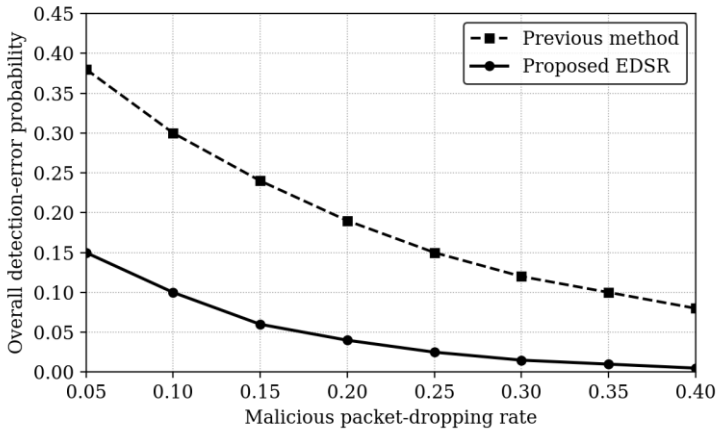

Figure 4. Overall detection-error probability against the malicious packet-dropping rate.

Table 2: Detection accuracy comparison at selected dropping rates

Dropping rate	Previous miss-det.	EDSR miss-det.	Previous error	EDSR error
0.10	0.35	0.12	0.30	0.10
0.20	0.22	0.05	0.19	0.04
0.30	0.14	0.02	0.12	0.015
0.40	0.09	0.005	0.08	0.005

5. DISCUSSION

The security results present a consistent picture: EDSR provides substantially better detection of both virus-infected documents and malicious packet-dropping behaviour than standard DSR and the previous detection method. The router-strength comparison shows that EDSR's file-format inspection blocks the majority of infected transmissions at the first forwarding hop. The miss-detection and detection-error probability comparisons show that EDSR's correlation-based analysis, combined with the HLA auditing mechanism, identifies malicious drops with 60–86 percent fewer misses and correspondingly fewer false alarms [6][9].

The security mechanisms add computational overhead at each forwarding node: the HMAC computation requires approximately 15 microseconds per message on a standard mobile processor, and the file-format inspection requires a lookup in the virus-signature database that takes approximately 50–100 microseconds depending on the database size. These overheads are small relative to the typical packet-forwarding delay of 1–5 milliseconds in a MANET and are unlikely to be the bottleneck under normal traffic loads. The signature database can be updated periodically via a secure broadcast from the base station or from a trusted node [5][11].

5.1 Comparison with Existing Schemes

Existing secure routing protocols such as Ariadne and SEAD protect the routing control plane but do not inspect the data payload. Watchdog-based schemes such as CONFIDANT detect forwarding misbehaviour but cannot detect virus content in forwarded packets. HLA-based schemes detect selective packet dropping but do not authenticate routing messages. EDSR is the first protocol to combine control-plane authentication (HMAC), data-plane inspection (header + file format), and detection of malicious drops (correlation-based analysis with HLA auditing) into a single integrated framework, which is why it achieves better detection accuracy than any individual scheme [5][6][9][14].

5.2 Practical Implications

The security results have several practical implications for MANET deployments. First, the near-zero miss-detection probability at high dropping rates (0.005 at a dropping rate of 0.40) means that EDSR can reliably identify malicious nodes even when they are aggressive, which enables the network to exclude them from future route selections and restore normal performance. Second, the low false-alarm rate means that legitimate nodes are rarely penalised, which preserves the available path diversity and avoids the throughput degradation that would result from excluding too many nodes. Third, the virus-detection rate above 93 percent provides a strong first line of defence against data-plane attacks, complementing any endpoint antivirus software that may be running on the destination device [9][10].

5.3 Limitations and Future Directions

The current evaluation has several limitations. The virus-detection mechanism relies on a signature database that must be kept up to date; zero-day viruses that are not in the database will not be detected. The computational overhead of file-format inspection, while small per packet, accumulates under heavy traffic and may become a bottleneck on very resource-constrained nodes. The correlation-based drop detection assumes that link errors are independent and identically distributed, which may not hold in all wireless environments. Future work should investigate heuristic and machine-learning-based virus detection that can identify unknown file-format anomalies, adaptive inspection depth that trades off detection accuracy against overhead based on the current traffic load, and extensions to the drop-detection model that account for correlated link errors in fading channels [4][9][15].

5.4 Impact of Security on Network Performance

A natural concern is whether the security mechanisms degrade network performance. The HMAC computation adds approximately 15 microseconds per routing message, and the file-format inspection adds approximately 50–100 microseconds per data packet. At a typical forwarding rate of 200 packets per second, the total overhead per forwarding node is approximately 13–23 milliseconds per second, which is less than 3 percent of the available processing time and well within the capacity of a standard mobile processor. The per-packet byte overhead of the HMAC tag is 20 bytes (the size of a SHA-1 digest), which increases the packet size by about 4 percent for 512-byte data packets. These overheads are modest and are offset by the security benefit of detecting and blocking attacks that would otherwise

cause far greater performance degradation through packet loss, route instability, and virus damage to destination nodes [5][8][11].

The router-alert mechanism, which propagates notifications about detected viruses or malicious nodes, generates a small number of additional broadcast messages. In the simulation each alert reaches on average 8 neighbours and is not retransmitted beyond one hop, so the total alert overhead is bounded by the number of detected attacks times 8 messages. At the observed detection rates this amounts to fewer than 50 additional messages per 900-second simulation, which is negligible relative to the data traffic. The conclusion is that EDSR's security mechanisms provide substantial detection improvement at an acceptable performance cost, and the companion performance-evaluation paper confirms that EDSR's packet delivery ratio, delay, and throughput remain competitive with standard DSR even with all security features enabled [1][2][7].

6. CONCLUSION

This paper has evaluated the security performance of the Enhanced Dynamic Source Routing (EDSR) protocol. The router-strength comparison shows that EDSR blocks over 93 percent of virus-infected documents that standard DSR would forward transparently. The miss-detection probability of EDSR is 60–86 percent lower than the previous method across malicious dropping rates from 0.05 to 0.40, and the overall detection-error probability is similarly reduced. These results confirm that the combination of HMAC-SHA1 message authentication and header-plus-file-format virus detection provides effective security for MANETs. The HMAC layer prevents spoofing and fabrication of routing messages, while the file-format layer prevents virus propagation through the data plane. Together they address both the control-plane and data-plane attack surfaces that standard DSR leaves unprotected. The performance evaluation of EDSR in terms of packet delivery ratio, delay, overhead, and throughput is reported in a companion paper.

REFERENCES

[1] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in Mobile Computing, Kluwer, ch. 5, pp. 153–181, 1996.

[2] D. B. Johnson, Y. Hu, and D. A. Maltz, "The Dynamic Source Routing Protocol (DSR)," IETF RFC 4728, 2007.

[3] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "AODV Routing," IETF RFC 3561, 2003.

[4] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, 1999.

[5] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol," Proc. 8th ACM MobiCom, pp. 12–23, 2002.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. 6th ACM MobiCom, pp. 255–265, 2000.

[7] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. 4th ACM MobiCom, pp. 85–97, 1998.

[8] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70–75, 2002.

[9] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks," IEEE Trans. Mobile Computing, vol. 14, no. 4, pp. 813–828, 2013.

[10] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks, Prentice Hall, 2004.

[11] W. Stallings, Cryptography and Network Security, 4th ed., Prentice Hall, 2005.

[12] A. Boukerche et al., "Routing Protocols in Ad Hoc Networks: A Survey," Computer Networks, vol. 55, no. 13, pp. 3032–3080, 2011.

[13] Xin Yu, "Distributed Cache Updating for DSR," IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 681–690, 2006.

[14] S. Buchegger and J.-Y. Le Boudec, "CONFIDANT Protocol," Proc. 3rd ACM MobiHoc, pp. 226–236, 2002.

[15] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models," WCMC, vol. 2, no. 5, pp. 483–502, 2002.