# Evaluating Energy Efficiency of Secure Routing Schemes for Mobile Ad-Hoc Networks

RUTVIJ H. JHAVERI
Research Scholar, Department of Computer Engineering, CSPIT, Charotar University of Science & Technology, Changa, Gujarat, India.
and
NARENDRA M. PATEL
Associate Professor, Department of Computer Engineering, Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar, Gujarat, India.

One of the primary concerns during the design of a secure routing protocol in Mobile Ad-hoc Networks (MANETs) is the balance between security and energy efficiency. Routing decisions play a vital role in secure data transmission and in balancing power consumption at the network layer in order to achieve Quality-of-Service (QoS) requirements in the network. This paper aims at evaluating the energy efficiency of different secure routing schemes addressing packet forwarding misbehavior in MANETs. The approaches are evaluated in NS-2 under distinct types of adversaries and under varying network conditions.

Keywords: MANET, packet forwarding misbehavior, security, secure routing schemes, energy analysis.

## 1. INTRODUCTION

Due to the promising characteristics of MANETs such as rapidly deployable wireless communication, ubiquitous computing and stable connectivity, they promise exciting applications in the upcoming years [Vasserman et al. 2013]. However, they are subject to some big challenges due to their dynamic topology, resource-constrained environment and shared wireless medium. A MANET usually consists of power-constrained mobile nodes and their lifetime largely depends on the efficient use of the power sources; power depletion of these nodes may lead to performance degradation, network partition or network failure [Liu et al. 2011]. Therefore, devising a strategy for efficient energy management is imperative for these unique decentralized networks.

In a MANET, where multi-hop communication takes place, each node acts not only as a host but also as a router to forward the packets for other nodes which are not in its communication range [Jhaveri et al. 2015b]. As a result, a node not only consumes energy while transmitting its own packets but also while forwarding packets of other nodes. Furthermore, energy is also drained by receiving or overhearing packets of other nodes. In such a power-constrained environment, a routing scheme should be carefully designed to reduce the energy cost of data communication in the network. At the same time, the routing scheme is also expected to take care of security aspect due to the limited physical security of MANETs [Subramaniyan et al. 2014] and absence of security considerations in the traditional routing protocols designed for ad-hoc networks. In the process of improving the security of a routing scheme, the designers should not neglect the energy aspect. Therefore, it is imperative that a routing protocol should perform balancing act between security and energy aspects in order to achieve better Quality-of-Services (QoS). A secure routing scheme might not turn out to be useful in practical use if it consumes objectionable amount of energy. In recent years, extensive research efforts have been devoted to devising energy efficient

Authors′ addresses: Rutvij H. Jhaveri, SVM Institute of Technology, Department of Computer Engineering, College Campus, Old N.H.-8, Bharuch-392001, Gujarat, India; Narendra M. Patel, Department of Computer Engineering, Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar-388120, Gujarat, India.

secure routing schemes.

In this work, we evaluate different secure routing schemes incorporated with Ad-hoc On-demand Distance Vector (AODV) routing protocol which attempt to mitigate packet forwarding misbehaviors in MANETs: (i) *Sequence Number based Bait Detection Scheme (SNBDS)* [Jhaveri et al. 2015a] uses a heuristic mechanism when a node observes suspicious route reply from its peer node. It heuristically predicts a suspicious node based on the values of the destination sequence number of the received route reply and that of the routing table, and current time. The suspicious node is confirmed as a malicious node by employing a bait addressing technique. Thus, the malicious nodes are detected during the route discovery phase. (ii) *Detection, Prevention and Reactive AODV (DPRAODV)* [Raj et al. 2009] is a heuristic scheme which attempts to isolate malicious nodes during route discovery phase based on the values of the destination sequence number of the received route reply and that of the routing table. Identities of the recorded blacklisted nodes are propagated throughout the network using a broadcast message. (iii) *Trusted Routing Scheme with Pattern Discovery (TRS-PD)* [Jhaveri et al. 2016], addresses the limitations of SNBDS. It integrates a mechanism to discover attack patterns on the top of the trust model. The trust model evaluates trust of a neighbor node using drop ratios of control packets and data packets. This mechanism enhances the routing process by predicting the neighbors future behaviors by observing them for attack patterns. (iv) *Dually Secured AODV (DSAODV)* [Patel et al. 2015] addresses packet forwarding misbehavior in MANETs with two tier security mechanism. During route discovery phase a malicious node is detected based on the routing table sequence number, number of route requests sent and number of route replies received. Another tier of security is added during the data transmission phase which detects malevolent neighbor nodes based on the number of data packets sent by a node and the number of data packets forwarded by its neighbor nodes. In this paper, we perform energy analysis of these four schemes under varying network conditions and under three distinct adversary models presented in [Jhaveri et al. 2016].

The remainder of this paper is organized as follows. Section 2 gives an overview of the existing energy efficient secure routing schemes for wireless ad-hoc networks. Section 3 describes the energy consumption model. Detailed working of the secure routing schemes is presented in Section 4. Section 5 presents the mode of operations of the three adversary models. The simulation results are presented in Section 6. Finally, Section 7 concludes the paper.

## 2. ENERGY EFFICIENT SECURE ROUTING SCHEMES

In this section, we provide studies related to existing energy efficient secure routing schemes.

Miglani et al. [2014] proposed a Power aware Secure Dynamic Source Routing (PS-DSR) protocol to detect packet dropping and packet modification attacks; this approach employs route selection based on trust values of the nodes in the route; it selects a set of nodes which act as monitoring nodes in their promiscuous mode to detect malicious nodes in the network; the approach is evaluated using metrics such as packet delivery ratio, packet loss, end-to-end latency, routing overhead and path optimality. An Energy-Efficient Scheme Immune to Wormhole attacks (E2SIW) proposed by Dhurandher et al. [2012] uses Global Positioning System (GPS) to observe location information of the nodes in order to detect hidden or participating wormhole nodes; it observes the routing variations between peer nodes along a route from the source to the destination node; an alternate route is found after the attack detection by bypassing the wormhole nodes; the protocol is claimed to be simple and localized; the performance of E2SIW is evaluated using metrics such as detection time, energy consumption, control packets transmitted and wormhole detection percentage. Alnumay et al. [2012] proposed a clustering-based energy aware secure routing protocol in which most trustworthy and energy-efficient node is selected as a cluster-head; the trust based scheme considers mobility and battery-power and ensures efficient intra-cluster and inter-cluster routing and secure packet delivery; the self and recommended evidences are combined using Dempster-Shafer (DS) mathematical model [Shafer et al. 1976]; network lifetime is selected as the metric for performance evaluation. Biswas et al. [2014] proposed a trust-based scheme to detect single and cooperative blackhole nodes; trust of a node is evaluated by mobility, pause time and residual energy and based on that, the most reliable route is selected for data transmission; however, the approach has drawback of false positives in certain scenarios; the approach is evaluated with metrics such as packet delivery ratio and battery utilization. Kukreja et al. [2015] proposed an Energy Efficient Secure Dynamic Source Routing (EESDSR) protocol to detect packet dropping activities, selfish nodes and malicious topology changing behavior; this trust based approach takes into account the dynamic topology, distributed nature and energy constraints of mobile nodes; monitor nodes are selected periodically all over the network; the information about the malicious node is propagated immediately after detection using a newly created control packet; the mechanism is evaluated using metrics such as packet delivery ratio, packet loss, end-to-end latency, routing overhead and path optimality. An energy-efficient multipath routing scheme based on a Markov chain proposed by Sarkar et al. [2016] attempts to mitigate jamming, interception and data hijacking attacks; packet forwarding energy cost is taken as a value function of a Markov chain to decide optimal routing strategy; an energy-efficient route is stochastically selected from the set of computed routes; moreover, data packets are forwarded through random routes in order to complicate the listening of packets by attackers; performance of the scheme is analyzed in terms of energy consumption, throughput, end-to-end delay and security.

## 3. ENERGY CONSUMPTION MODEL

The radio of a wireless node in a MANET can be either in awake state or sleep state. There are three modes in the Awake state: Transmit, Receive and Idle (Standby); each mode consumes a different level of energy [Mahfoudh et al. 2010]. Sleep state consumes very small amount of energy as compared to Awake state [Lee et al. 1996]. Based on the study shown in [Mahfoudh et al. 2010] and [Walikar et al. 2015], we adopt the following energy consumption model to compute the average remaining energy of a node. We use the following notations as shown in Table I:

Table I: Explanation of the notations

| **Notations** | **Meaning** |
|---|---|
| $n_i$ | A mobile node in the MANET with identity i |
| T | Time for handling a packet |
| S | Size of a packet |
| $E_{TX}$ | Energy consumed in transmitting operation |
| $E_{RX}$ | Energy consumed in reception operation |
| $P_{TX}$ | Transmission power |
| $P_{RX}$ | Receiving power |
| $E_{IDLE}$ | Energy consumed in idle mode |
| $E_{SLEEP}$ | Energy consumed in sleep mode |
| $E_{TRANS}$ | Energy consumed during transition from one state to another |
| $EI_i$ | Initial energy of the node $n_i$ |
| $EC_{i(t)}$ | Energy consumed by the node $n_i$ till time t |
| $ER_{i(t)}$ | Residual energy of the node $n_i$ at time t |
| $EC_{N(t)}$ | Average energy consumed in the network at time t |
| TP | Total number of transmitted packets |
| RP | Total number of received packets |

Consider a MANET of $m$ homogenous mobile nodes, which can be denoted as:

$$N = \{n_1, n_2, n_3, \ldots n_m\} \tag{1}$$

The energy consumed can be computed by the following equation:

$$Energy = Power \times Time \tag{2}$$

The time $T$ for handling a packet of size $S$ can be computed by:

$$T = \frac{S \times 8}{Bandwidth} \tag{3}$$

The energy consumed by a node in transmitting a packet, can be computed by:

$$E_{TX} = P_{TX} \times T \tag{4}$$

The energy consumed by a node in receiving a packet, can be computed by:

$$E_{RX} = P_{RX} \times T \tag{5}$$

The total energy consumed by a node $n_k$ till time $t_j$ can be represented by:

$$EC_k(t_j) = (E_{TX} \times TP) + (E_{RX} \times RP) + E_{IDLE} + E_{SLEEP} + E_{TRANS} \tag{6}$$

Therefore, the residual energy of $n_k$ after time $t_j$ can be represented by:

$$ER_k(t_j) = EI_k - EC_k(t_j) \tag{7}$$

The average energy consumed by a node in the network at time $t_j$, can be represented by:

$$EC_N(t_j) = \frac{\sum_{i=1}^{m} EC_i(t_j)}{m} \tag{8}$$

## 4. SECURE ROUTING SCHEMES

A variety of attacks can be launched on MANET routing protocols to degrade the network performance. Compromised nodes may perform various kinds of packet forwarding misbehaviors which in turn affect the QoS of the network. In this paper, we analyze energy efficiency of four secure routing schemes which address this issue.

### 4.1 SNBDS

SNBDS [Jhaveri et al. 2015a] is a heuristic scheme which attempts to isolate malicious nodes during the route discovery process. It uses bait addressing technique to verify the existence of a misbehaving node; this technique is useful when a malicious node receives a request and immediately sends a forged reply for the destination for which it does not have a route in the routing table. The operations performed by a node adopting SNBDS to mitigate packet forwarding misbehavior are described herewith:

*Step 1*: After receiving a route reply, calculate the difference between the destination sequence number of the route reply and that of the routing table.

*Step 2*: Calculate the maximum value of the recorded difference between the sequence numbers of the received route reply and that of the routing table (denoted as *max_diff*), amongst all routing table entries.

*Step 3*: Calculate the maximum sequence number frequency increments till current time.

*Step 4*: Heuristically calculate the maximum possible difference between the sequence numbers of the received reply and that of the routing table (denoted as *h_max_diff*) using the maximum sequence number increment frequency, current time and time of the last received reply.

*Step 5*: Calculate a threshold value of the maximum possible difference between the sequence numbers of the received reply and that of the routing table by finding the maximum of *max_diff* and *h_max_diff*.

*Step 6*: If the difference between the destination sequence numbers of the route reply and that of the routing table is greater than the threshold, mark the node sending reply packet as a suspicious node and buffer its reply packet.

*Step 7*: Send a bait request with forged destination identity and forged sequence number to the suspicious node.

*Step 8*: If a reply is received from the suspicious node for the bait request, mark that node as a

malicious node and drop its buffered reply packet.
*Step 9*: Append a list of the recorded malicious nodes to route request packet in order to propagate their identities in the network.
*Step 10*: Isolate the malicious nodes during future route construction process by dropping all packets received from them.

### 4.2 DPRAODV

DPRAODV [Raj et al. 2009] is a heuristic scheme which attempts to isolate malevolent nodes during the route discovery phase. It uses a dynamic threshold value to detect misbehaving nodes which is updated after specific time interval. All nodes sending route reply packets with sequence number greater than the threshold value are marked as malicious nodes. Identities of the malicious nodes are propagated in the network through broadcasted messages. The operations performed by a node adopting DPRAODV to mitigate packet forwarding misbehavior are described herewith:
*Step 1*: After receiving a route reply, calculate a threshold value by finding the average of the difference between the destination sequence numbers of the route reply packet and that of the routing table in each time slot.
*Step 2*: If the difference between the destination sequence numbers of the route reply and that of the routing table is greater than the threshold, mark the node sending reply packet as a malicious node and discard the reply packet.
*Step 3*: Build a blacklist containing the identities of the recorded malicious nodes.
*Step 4*: Broadcast an *alarm* packet containing the blacklist in order to inform other nodes in the network about the misbehaving nodes.
*Step 5*: Isolate the malicious nodes during future route establishment process by dropping all packets received from them.

### 4.3 TRS-PD

TRS-PD [Jhaveri et al. 2016] is a trust-based scheme which attempts to eradicate the limitations of SNBDS [Jhaveri et al. 2015a]. The scheme integrates the model of *Method of Common Differences (MCD)* on the top of the trust-model to discover the malicious patterns generated by intelligent adversaries. A node records the required field values of the received and overheard control packets on a regular basis. The operations performed by a node during the trust-update interval to mitigate packet forwarding misbehavior by neighbor nodes are described herewith:
*Step 1*: Verify the existence of attack patterns followed by the neighbor with the help of the recorded field values using the model of *MCD*.
*Step 2*: Calculate the distrust value of the neighbor using the number of dropped control and data packets.
*Step 3*: If the neighbor follows an attack pattern or has the distrust value greater than the threshold value, record it as a malicious node in the neighbor table.
*Step 4*: If a routing table entry exists with its next hop as a malicious node, discard the entry and initiate a local route discovery process to find an alternate path to the destination (route-handoff).
*Step 5*: If a node brings its distrust value less than the threshold value and, if it does not follow any attack pattern and recommended as trusted node by neighbors then it is recorded as a benevolent node in its neighbor table entry.
*Step 6*: Send trust recommendations of neighbors by broadcasting *HELLO* packets.

### 4.4 DSAODV

DSAODV [Patel et al. 2015] contains two tier security mechanisms in order to detect packet forwarding misbehavior. During route discovery process, a malicious node is detected if the sequence number in the received reply packet crosses a threshold value constructed by adding the routing table sequence number, number of route requests sent and number of route replies received. On the other hand, if a neighbor node drops the data packets beyond a threshold value,

it is marked as a malicious node during data transmission process. The operations performed by a node adopting DSAODV to mitigate packet forwarding misbehavior are described herewith:
*Step 1*: After receiving a route reply, calculate a threshold value by finding the sum of the routing table sequence number, number of route requests sent and number of route replies received.
*Step 2*: If the destination sequence number of the route reply is greater than the threshold, mark the node sending reply packet as a malicious node and discard the reply packet.
*Step 3*: Monitor the neighbor nodes for their packet dropping activities.
*Step 4*: If packet loss by a neighbor node crosses a threshold value, mark the neighbor node as a malicious node.
*Step 5*: Build a blacklist containing the identities of the recorded malicious nodes.
*Step 6*: Broadcast an alarm packet containing the blacklist in order to inform other nodes in the network about the misbehaving nodes.

### 4.5 Comparision between the Security Schemes

The key differences between SNBDS, DPRAODV, TRS-PD and DSAODV are listed out in Table II.

Table II: Comparison of the security schemes

| **SNBDS** | **DPRAODV** | **TRS-PD** | **DSAODV** |
|---|---|---|---|
| Heuristic approach | Heuristic approach | Trust-based approach | Hybrid approach |
| Uses bait addressing technique | Uses dynamic threshold mechanism | Uses attack pattern discovery technique | Uses two tier security mechanism |
| Deciding factors: Destination Sequence Number, Time | Deciding factor: Destination Sequence Number | Deciding factors: Destination Sequence Number, Time, Hop Count, Control and Data packet drops | Deciding factor: Destination Sequence Number, Number of Route Requests and Route Replies, Packet loss |
| Works during route discovery process | Works during route discovery process | Works during route discovery and data transmission processes | Works during route discovery and data transmission processes |
| Does not use local route discovery process | Does not use local route discovery process | Uses local route discovery process | Does not use local route discovery process |
| Uses route request packet to propagate information about malicious nodes | Introduces an alarm packet to propagate information about malicious nodes | Uses HELLO messages to provide trust recommendations to the neighbor nodes | Introduces an alarm packet to propagate information about malicious nodes |

## 5. ADVERSARY MODELS

We evaluate the energy efficiency of the aforementioned schemes against three distinct adversary models as described in [Jhaveri et al. 2016].

### 5.1 First Adversary Model

The operations of this *intelligent adversary* (denoted as *Attack1*) are described below:
*Step 1*: Operate in promiscuous mode to record the highest value of the destination sequence number from the received or overheard control packets.
*Step 2*: If a route request is received, discard it and check the availability of the route in the routing table.
*Step 3*: If a valid fresher route exists in the routing table, send a route reply with incremented value of the highest recorded sequence number and with hop count 2.
*Step 4*: Start dropping the data packets till 50% of the time period after the first packet is received from the source node.

The adversary follows a pattern by constantly sending identical hop count value.

### 5.2 Second Adversary Model

The operations of this *slow poison adversary* (denoted as *Attack2*) are described below:
*Step 1*: If a route request is received, discard it.
*Step 2*: Send a route reply with incremented value of the sequence number in route request and with a random hop count value.
*Step 3*: After receiving the first data packet, drop the packets according to the Fibonacci sequence as per the time slot. e.g. 0 packet in first time slot, 1 in second, 1 in third, 2 in fourth and so on.

The adversary follows a pattern by constantly sending incremented value of destination sequence number of the received route request packet.

### 5.3 Third Adversary Model

The operations of this *capricious adversary* (denoted as *Attack3*) are described below:
*Step 1*: If a route request is received, discard it.
*Step 2*: Send a route reply with random values of the sequence number (marginally higher) and hop count.
*Step 3*: Drop the data packets in a random manner during the life span of the network.

The adversary adopts random behavior during route discovery and data transmission phases and, doesn′t follow any attack pattern.

## 6. SIMULATION RESULTS AND ANALYSIS

We evaluate the performance efficiency of SNBDS and TRS-PD against Attack1, Attack2 and Attack3 using NS-2 (ver. 2.34) network simulator under the Linux system. We simulate a MANET with 50 mobile nodes adopting IEEE 802.11 MAC protocol; the nodes adopt random way point mobility model. Randomly located malicious nodes perform packet forwarding misbehavior by launching either *Attack1* or *Attack2* or *Attack3*. Node pairs are randomly selected to generate CBR-UDP traffic where packets are sent at the rate of 4 packets/s. Each simulation result is an average value resulting from 10 different simulation runs. We consider that the wireless network interface consumes 1.65 W, 1.4 W, 1.15 W and 0.045 W for the *Transmit*, *Receive* and *Idle* modes and the *Sleep* state, respectively [Van der Moolen et al. 1998], [Jung et al. 2002]. 800$\mu$s is taken as the transition time from the *Sleep* state to *Awake* state and during this transition time, a mobile node will consume 2.3 W power (double than the *Idle* mode) [Jung et al. 2002]. Table III presents the major simulation parameters.

The performances of the secure routing schemes are evaluated using the *Average Energy Consumption* metric under varying mobility and varying percentage of malicious nodes.

### 6.1 Test1: Varying Node Mobility

In this test, we compare the performance of the secure routing schemes under Attack1, Attack2 and Attack3 by varying mobility of nodes from 4 m/s to 20 m/s. The number of malicious nodes is kept to 20% and other parameters are kept fixed.

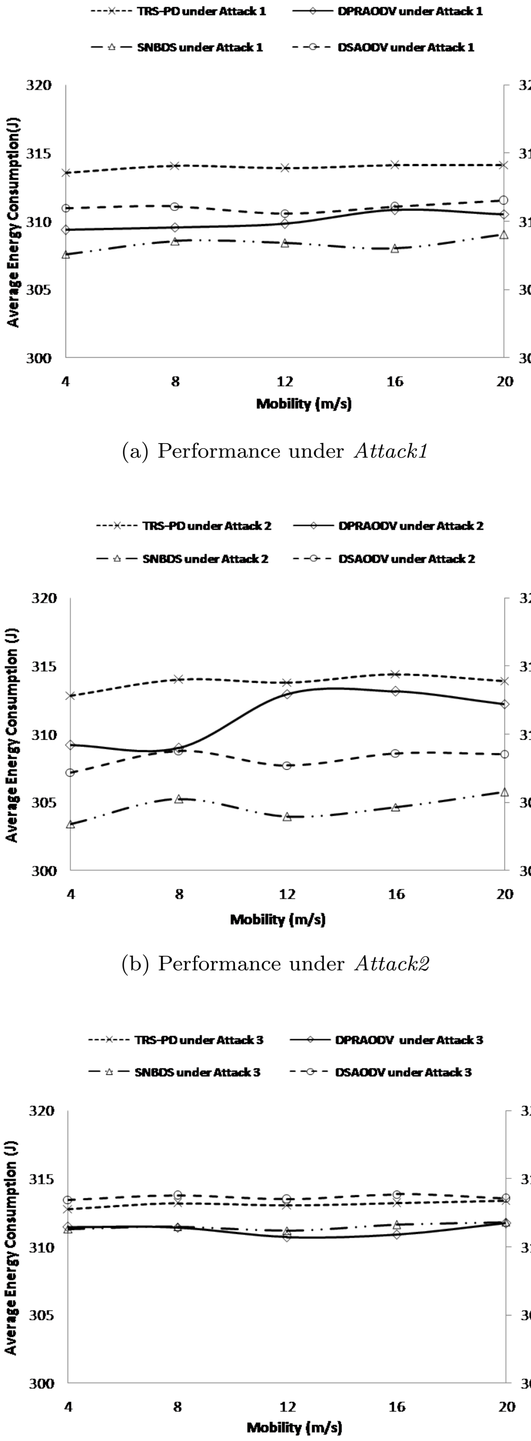
As shown in Fig. 1, the average energy consumption of the network is different under the distinct adversary models. As depicted by the graph in Fig 1. (a), the average energy consumption under Attack1 varies between 307.58 J and 309.02 J for SNBDS, while it varies between 309.35 J and 310.82 J for DPRAODV, 313.56 J and 314.13 J for TRS-PD, and 310.56 J and 311.50 J for DSAODV. TRS-PD consumes the highest amount of energy while SNBDS consumes the lowest amount of energy. The average difference of the average energy consumption between TRS-PD and DSAODV is 2.92 J, between DSAODV and DPRAODV is 1.02 J, and between DPRAODV and SNBDS is 1.70 J.

Table III: Simulation Parameters

| **Parameter** | **Value** |
|---|---|
| Coverage area | 1000 m × 1000 m |
| Communication range | 250 m |
| Channel bandwidth | 2 Mbps |
| Packet size | 512 bytes |
| Simulation duration | 240 s |
| Number of nodes | 50 |
| Maximum mobility | 4 m/s ∼ 20 m/s |
| Pause time | 5 s |
| Number of connections | 15 |
| Percentage of malicious nodes | 0% ∼ 40% |
| Routing protocols | SNBDS, DPRAODV, TRS-PD, DSAODV, Attack1, Attack2, Attack3 |
| Initial energy | 1000 J |
| Transmit power | 1.65 W |
| Receive power | 1.4 W |
| Idle power | 1.15 W |
| Sleep power | 0.045 W |
| Transition power | 2.3 W |
| Transition time | 800$\mu$s |

As depicted by the graph in Fig 1. (b), the average energy consumption under Attack2 varies between 303.40 J and 305.74 J for SNBDS, while it varies between 308.98 J and 313.13 J for DPRAODV, 312.82 J and 314.40 J for TRS-PD, and 307.20 J and 308.76 J for DSAODV. TRS-PD consumes the highest amount of energy while SNBDS consumes the lowest amount of energy. The average difference of the average energy consumption between TRS-PD and DPRAODV is 2.49 J, between DPRAODV and DSAODV is 3.13 J, and between DSAODV and SNBDS is 3.57 J.

As depicted by the graph in Fig 1. (c), the average energy consumption under Attack3 varies between 311.19 J to 311.82 J for SNBDS, while it varies between 310.71 J and 311.72 J for DPRAODV, 312.79 J and 313.41 J for TRS-PD, and 313.46 J and 313.86 J for DSAODV. DSAODV consumes the highest amount of energy while DPRAODV consumes the lowest amount of energy in most cases. The average difference of the average energy consumption between DSAODV and TRS-PD is 0.49 J, between TRS-PD and SNBDS is 1.64 J, and between SNBDS and DPRAODV is 0.24 J.



(a) Performance under *Attack1*

(b) Performance under *Attack2*

(c) Performance under *Attack3*

Figure. 1: Performance comparison by varying speeds of nodes.

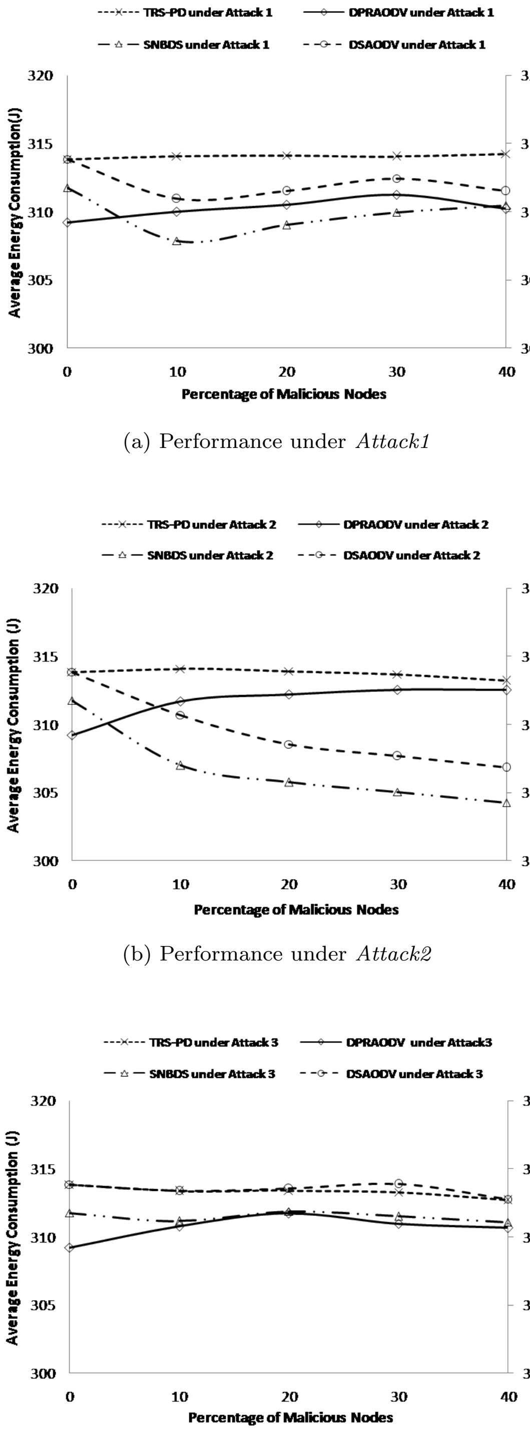
### 6.2 Test2: Varying Percentage of Malicious Nodes

In this test, we compare the performance of the secure routing schemes under Attack1, Attack2 and Attack3 by varying number of malicious nodes from 0% to 40%. The maximum speed of nodes is kept to 20 m/s and other parameters are kept fixed.

As shown in Fig. 2, the average energy consumption of the network is different when distinct types of adversaries compromise the network. As depicted by the graph in Fig 2. (a), in the presence of adversaries, the average energy consumption under Attack1 varies between 307.85 J and 310.45 J for SNBDS, while it varies between 310.01 J and 311.25 J for DPRAODV, 314.04 J and 314.25 J for TRS-PD, and 310.95 J and 312.45 J for DSAODV. TRS-PD consumes the highest amount of energy while SNBDS consumes the lowest amount of energy in the presence of adversaries. The average difference of the average energy consumption between TRS-PD and DSAODV is 2.53 J, between DSAODV and DPRAODV is 1.10 J, and between DPRAODV and SNBDS is 1.18 J in the presence of adversaries.

As depicted by the graph in Fig 2. (b), in the presence of adversaries, the average energy consumption under Attack2 varies between 304.24 J and 306.99 J for SNBDS, while it varies between 311.71 J and 312.54 J for DPRAODV, 313.20 J and 314.08 J for TRS-PD, and 306.82 J and 310.68 J for DSAODV. TRS-PD consumes the highest amount of energy while SNBDS consumes the lowest amount of energy in the presence of adversaries. The average difference of the average energy consumption between TRS-PD and DPRAODV is 1.47 J, between DPRAODV and DSAODV is 3.82 J, and between DSAODV and SNBDS is 2.93 J in the presence of adversaries.

As depicted by the graph in Fig 2. (c), in the presence of adversaries, the average energy consumption under Attack3 varies between 311.08 J to 311.88 J for SNBDS, while it varies between 310.65 J and 311.72 J for DPRAODV, 312.68 J and 313.41 J for TRS-PD, and 312.76 J and 313.87 J for DSAODV. DSAODV consumes the highest amount of energy while DPRAODV consumes the lowest amount of energy in the presence of adversaries. The average difference of the average energy consumption between DSAODV and TRS-PD is 0.20 J, between TRS-PD and SNBDS is 1.78 J, and between SNBDS and DPRAODV is 0.38 J in the presence of adversaries.



(a) Performance under *Attack1*

(b) Performance under *Attack2*

(c) Performance under *Attack3*

Figure. 2: Performance comparison by varying percentage of malevolent nodes.

## 7. CONCLUSIONS

It is imperative to consider security and energy aspects during the design of a routing protocol. There exist many security schemes which attempt to improve one aspect by compromising the other one. In this paper, we analyze the energy efficiency of different secure routing schemes. The experimental results in this work depict that the average energy consumption of TRS-PD and DSAODV is always higher than that of other heuristic schemes. Thus, detection of malicious nodes during data transmission phase leads to higher energy consumption than that during route discovery phase. It can be concluded that a suitable secure routing scheme should be selected on the basis of the specific security requirements and QoS constraints of the network.

## ACKNOWLEDGMENTS

The authors would like to thank the management of Charotar University of Science & Technology (CHARUSAT), Changa, India and the management of SVM Institute of Technology, Bharuch, India for providing the necessary resources to complete this work. Special thanks go to Prof. (Dr.) D.C. Jinwala of SVNIT, Surat, India, Prof. (Dr.) Robert van Glabbeek of NICTA, Australia and Charles Perkins of Nokia Research, USA for their able guidance and motivation. The authors are grateful to the anonymous reviewers.

## REFERENCES

Alnumay, W. S.,Chatterjee, P., and Ghosh, U. 2014. Energy aware secure routing for wireless ad hoc networks. IETE Journal of Research 60, 1 (2014), 50-59.

Biswas, S., Nag, T. and Neogy, S. 2014. Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In *Proceedings of the Applications and Innovations in Mobile Computing (AIMoC), (2014). 157-164.*

Dhurandher, S.K., Woungang, I., Gupta, A., and Bhargava, B.K. 2012. : E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks. In *Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA),(2012). 472-477.*

Jhaveri, R.H., and Patel, N.M. 2015a. A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wireless Networks 21, 8 (2015a), 2781-2798.

Jhaveri, R.H., and Patel, N.M. 2015b. Mobile ad-hoc networking with aodv: A review. International Journal of Next-Generation Computing 6, 3 (2015b), 165-191.

Jhaveri, R.H., and Patel, N.M. 2016. Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. International Journal of Communication Systems (2016).

Kukreja, D., Dhurandher, S.K., and , Reddy, B.V. 2015. Enhancing the security of dynamic source routing protocol using energy aware and distributed trust mechanism in manets. Intelligent Distributed Computing (2015), 83-94.

Liu, W., Zhang, C., Yao, G.,and Fang, Y. 2011. DELAR: a device-energy-load aware relaying framework for heterogeneous mobile ad hoc networks. IEEE Journal on Selected Areas in Communications 29, 8 (2011), 1572-1584.

Mahfoudh, S., and Minet, P. 2010. : Energy-aware routing in wireless ad hoc and sensor networks. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference,(2010). 1126-1130.*

Miglani, M., Kukreja, D., Dhurandher, S.K., and Reddy, B.V. 2014. Power aware and secure dynamic source routing protocol in mobile ad hoc networks. Security in Computing and Communications (2014), 45-56.

Patel, A.D., and Chawda, K. 2015. Dual security against grayhole attack in manets. Intelligent computing, communication and devices(2015), 33-37.

Raj, P.N., and Swadas, P.B. 2009. Dpraodv:A dyanamic learning system against blackhole attack in aodv based manet. International Journal of Computer Science Issues 2 (2009), 54-59.

Sarkar, S., and Datta, R. 2016. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Networks 37 (2016), 209-227.

Shafer, G. 1976. A mathematical theory of evidence (Vol 1). Princeton: Princeton university press (1976).

Subramaniyan, S., Johnson, W., and Subramaniyan, K. 2014. A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking 2014, 1 (2014), 1-10.

van der Moolen, W. 1998. IEEE 802.11 WaveLAN PC Card User′s Guide. Lucent Technologies (1998).

VASSERMAN, E.Y., AND HOPPER, N. 2013. Vampire attacks: Draining life from wireless ad hoc sensor networks. IEEE Transactions on Mobile Computing 12, 2 (2013), 318-332.

WALIKAR, G.A., AND BIRADAR, R.C. 2015. : Energy aware multicast routing in mobile ad-hoc networks using NS-2. In *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT),(2015). 1-7.*

LEE, Y.C.B., AND YOUN, H.Y. 1996. Power management in mobile computing. Technical report, University of Pennsylvania (1996).

**Rutvij H. Jhaveri** Rutvij H. Jhaveri is a Ph.D. scholar in the Department of Computer Engineering, CSPIT, CHARUSAT University, Changa, India. He has completed his Masters degree in Computer Engineering from Saradar Vallabhbhai National Institute of Technology, Surat and Bachelor of Engineering from Birla Vishvakarma Mahavidyalaya, V.V.Nagar in India. Since 2002, he is working as an Assistant Professor in SVM Institute of Technology, Bharuch, India affiliated to Gujarat Technological University.
He serves as a reviewer in high quality journals such as *Telecommunication Systems (Springer)*, *Wireless Networks (Springer)*, *The Computer Journal (Oxford)*, *International Journal of Advanced Computer Science and Applications (SAI)* and many more. He also serves as a program committee member/reviewer in renowned International conferences. He serves as an editorial board member in journals such as European Journal of Scientific Research and OMICS group of journals. He authored several papers/book-chapter(s) published by prominent publishers such as Wiely, Springer, Elsevier, IET, IEEE and Perpetual Innovation. He is also a member of various technical organizations such as ISTE, IDES, IACSIT, ICST and others. His papers have received 415+ peer citations as of June, 2016. His research interests include *issues and challenges in wireless ad-hoc networks* and *information security.*

**Narendra M. Patel** received his B.E. degree in electronics engineering from M.S. University, Baroda in 1993 and M.E. degree from M.S.University, Baroda in 1997. He received Ph.D degree from SVNIT, Surat in 2012. He is currently Associate Professor in Computer Engineering Department, B.V.M. Engineering College, V.V.Nagar, India. His research interests include *Digital Image Processing, Real Time Operating Systems, Distributed Systems* and *Computer Graphics.* He authored more than 45 papers which are published in prominent international journals and conference proceedings. He has guided more than 50 Master′s dissertations in Computer Engineering.