SPECIAL SECTION ON NEW TRENDS IN BRAIN
SIGNAL PROCESSING AND ANALYSIS

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 29, 2018, accepted January 17, 2019, date of publication January 29, 2019, date of current version February 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2896001

Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks

T. POONGODI[1], MOHAMMED S. KHAN[2], (Member, IEEE), RIZWAN PATAN[1], AMIR H. GANDOMI[3], AND BALAMURUGAN BALUSAMY[1]

[1]School of Computing Science and Engineering, Galgotias University, Greater Noida 201306, India
[2]Department of Computing, East Tennessee State University, Johnson, TN 37614-1266, USA
[3]School of Business, Stevens Institute of Technology, Hoboken, NJ 07030, USA

Corresponding author: Mohammed S. Khan (KHANMS@mail.etsu.edu)

ABSTRACT Performance and security are two critical functions of wireless ad-hoc networks (WANETs). Network security ensures the integrity, availability, and performance of WANETs. It helps to prevent critical service interruptions and increases economic productivity by keeping networks functioning properly. Since there is no centralized network management in WANETs, these networks are susceptible to packet drop attacks. In selective drop attack, the neighboring nodes are not loyal in forwarding the messages to the next node. It is critical to identify the illegitimate node, which overloads the host node and isolating them from the network is also a complicated task. In this paper, we present a resistive to selective drop attack (RSDA) scheme to provide effective security against selective drop attack. A lightweight RSDA protocol is proposed for detecting malicious nodes in the network under a particular drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANETs such as AODV and DSR. It accomplishes reliability in routing by disabling the link with the highest weight and authenticate the nodes using the elliptic curve digital signature algorithm. In the proposed methodology, the packet drop rate, jitter, and routing overhead at a different pause time are reduced to 9%, 0.11%, and 45%, respectively. The packet drop rate at varying mobility speed in the presence of one gray hole and two gray hole nodes are obtained as 13% and 14% in RSDA scheme.

INDEX TERMS Wireless ad-hoc networks, resistive to selective drop attack, network security, elliptic curve digital signature algorithm.

I. INTRODUCTION

Wireless Ad-Hoc Networks(WANETs) [1] decentralized nature makes suitable for different types of applications, where central nodes cannot be trusted on and may progress the scalability of networks linked to wireless networks, through practical and theoretical confines to the overall size of such networks have been recognized. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies in military or natural disasters conflicts. The existence of adaptive and dynamic routing protocol enables ad hoc networks to be formed quickly. The applications can further classify wireless Ad-hoc networks into Vehicular Ad hoc Networks (VANETs) [2], Mobile Ad hoc Networks (MANETs), Smartphone Ad-hoc Networks (SPANs) [3], Wireless mesh networks [4] and so on. The packet drop attack [5] can frequently be used to attack WANETs. The illustration of WANETs is shown in figure 1. Wireless networks have many different architectures than that of a typical wired network; a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host can drop packets at will [6]. Also over a mobile ad-hoc network, hosts are especially vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network [7]. The RSDA protocol can provide resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination. To address the selective drop attack [5], a reliable factor is chosen by computing the list of link weights. If the sum of the weight of a particular route is high, e.g., it indicates that the low reliability [8], the attacking node can be identified.

The associate editor coordinating the review of this manuscript and approving it for publication was Victor Hugo Albuquerque.

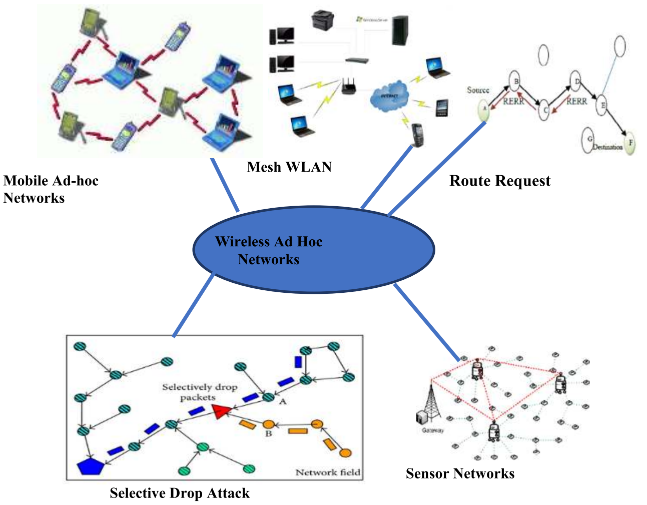

FIGURE 1. Wireless Ad-Hoc networks (WANETs).

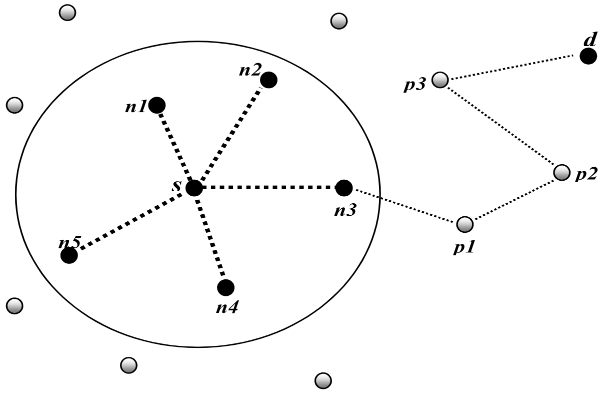

FIGURE 2. Failed or selfish node.

Each node maintains its own weight; the obtained weight is added to the route request payload. By computing the reliability rate, malicious nodes can be distinguished from other normal nodes. The performance of RSDA protocol is increased compared to existing approaches by considering the factors such as packet drop rate, jitter and routing overhead.

Node Detection [9]: Failure of a node would have an impact on the routing packets. Hence, such type of nodes should be detected and isolated to avoid network partitioning, which in turn affect thesurvival of the network. The failed node can typically be detected using routing protocols.

Node Isolation: The steps have been described for node isolation by considering the following scenarios,

Effect of Failed and Selfish Node: If the node n_3 is a failed node and if a node s starts a route discovery process to node d, the failed node n_3 cannot forward the packets received from the downstream nodes. If neighbors of node s are failed, then s would be unable to communicate with other nodes. Hence, the node s is said to be isolated by all its neighbors. If the node n_3 is taken as a selfish node as shown in figure2, when node s starts a route discovery process to node d, the selfish node n_3 may be reluctant to forward the request from s. In this case, n_3 behaves like a failed node. The node n_3 may discard data packets and forwards only control packets which are forwarded to it. Thus, the communication [10] between s and d is not ensured. If the neighbors of s are selfish, s would not be capable of communicating with other nodes, which are at one hop distance. Although the selfish nodes can still communicate with the remaining nodes, it is distinguished from the failed node.

The RSDA protocol has been designed to offer resistance to selective drop attacks by preventing the nodes from getting overloaded. It achieves reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination. This paper mainly contributes a discussed study on Wireless Ad Hoc Networks and their security related issues. A review on various protocols is done to deal with selective drop attack in WANET.A light weight RSDA protocol has been proposed for detecting malicious nodes in the network under selective drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANET such as AODV and DSR [39], [40].

An efficient cryptographic technique ECDSA has been chosen for providing authentication which has a lesser key size however it provides similar security. Finally, it achieves extreme network security measures ensures the integrity, availability, and performance enhanced using RSDA for WANET. This paper provides an overview of Wireless Ad hoc Networks and is organized as follows. In section 2, the previous work for selective drop attack is discussed. The theoretical approach to resolve the selective drop attack is explained in section 3. In section 4, the experimental setup and implementation details are discussed in detail. Section 5 presents the simulation results. Conclusion and future work are given in section 6.

II. RELATED WORK

Cho *et al.* [12] proposed the soft security mechanism as a fully distributed trust-based public key management technique for MANET. Instead of using hard security approaches to eliminate security vulnerabilities, the work aimed at maximizing the performance by relaxing security requirements focusing on the perceived trust. A Composite Trust-based Public Key Management (CTPKM) was proposed to maximize the performance by mitigating the vulnerabilities. A trusted threshold was fixed with each node to decide whether to trust another node or not.

Friginal *et al.* [13] proposed a security framework named Resilience Evaluation Framework for Ad Hoc routing protocols (REFRAHN) based on the insertion of malicious faults and quantitatively evaluated their effect on routing protocols. The primary goal of REFRAHN is to (i) minimize the uncertainty in the sources while deploying ad hoc routing protocols, (ii) devise fault-tolerant mechanisms that tackle and reduce such problems, and (iii) compare and choose the routing protocol that optimizes the robustness and performance of the network. Methodological aspects regarding fault injection in routing protocols have been extensively analyzed.

Ferraz *et al.* [14] proposed a robust and distributed access control mechanism depending on a trust model for securing the network and encouraging good cooperation by isolating misbehaving nodes in the network. The access control responsibility is viewed in two different contexts namely the local and global. In the local context responsibility, the neighbor nodes are intimated to notify about the suspicious behavior of the global context. While the global context examines the gathered information, a decision would be made to penalize the malicious node using a voting scheme. It was experimentally proven that the combination of voting, trust schemes offered a precise, accurate classification and node exclusion mechanism even in scenarios of limited monitoring.

Xia *et al.* [15] described the ad hoc network would function well only if the nodes are trustworthy and good cooperating. A dynamic trust prediction model is presented for evaluating the trustworthiness of nodes depend on nodes historical and future behavior by using extended fuzzy logic rules [16]. Moreover, the proposed trust prediction model is combined with a source route mechanism. The novel technique named Trust-based Source Routing protocol (TSR) [7] offers a flexible, feasible approach for choosing the shortest path by meeting the security requirement of packet transmission. TSR improves packet delivery ratio and reduces average end-to-end latency by conducting more experiments in malicious node detection and attack resistance.

Boppana and Su [17] focused on Anti Black Hole (ABM) mechanism, which estimates the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. Intrusion Detection System (IDS) nodes were employed in MANET to identify and prevent selective black hole attacks. If an intermediate node is not the destination and never broadcasts RREQ for a particular route, but forwards an RREP for the route, then its suspicious value would be incremented by 1 in the nearby IDS node's suspicious node table. When the suspicious value of a node exceeds a threshold, a block message is broadcasted by the IDS node to all remaining nodes in the network to isolate the suspicious node cooperatively [42]. Using ABM procedure, the IDS nodes deployed in sniff mode were used to estimate a suspicious value of a node based on its abnormal behavior during the transmission process. If the estimated value was found exceeding, then the IDS located nearby initiated the broadcasting of block message which in turn sends a notification message to all nodes such that all nodes in the network must carry out the isolation process in a cooperative manner. During the route discovery process, the gray hole nodes actively participate by forwarding RREQ packets for discovering a route to the destination. If such route established over the gray hole node, packets would be dropped selectively. Thus, gray hole nodes are not detected effectively by the approach.

Yu *et al.* [18] applied secured technique based on the reputation evaluation scheme in ad hoc networks. The behavior and correlation of the node were considered for building the reputation relation. The reputation evaluation technique was found to promote the cooperation of cluster members while forwarding data packets [19].

Komninos *et al.* [20] focused on randomly selecting intermediate nodes in the forwarding path as checkpoint nodes for sending acknowledgments for the received packets. If any misbehavior is detected, alarm packet is generated for transmitting information to the source node about the suspected activities. The scheme was observed to endure huge overhead since of sending acknowledgment reverse to the source node for the entire received packets by intermediate nodes.

Deng *et al.* [3] proposed a mechanism based on the simple rate-based control packet forwarding mechanism to alleviate malicious control packet. The proposed protocol was made secure against other DDoS attacks [21], and those legitimate nodes are not erroneously treated as misbehavior node. However, in the proposed mechanism, the distinguishing features of genuine and forged RREQs from the malicious or victim nodes were not differentiated.

Karlof and Wagner [22] used multipath forwarding technique to identify attacks in a wireless sensor network based on selective forwarding attack procedure. The attackers were not detected and isolated from the network efficiently.

The RSDA protocol has been proposed to offer resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing by disabling the link as defective or attempts to obtain a new efficient route to the destination. RSDA provides an effective security for selective drop attack. The attacker nodes can potentially drop the throughput of a host to the minimum level, and those nodes have been detected based on ECDSA [11]. The lightweight solution to selective drop attack has been provided by proposing RSDA protocol resists selective drop attacks by preventing the nodes from getting overloaded. Reliability is achieved in routing by rendering the link as defective or attempts to acquire an efficient route to the destination. RSDA assists in maximizing the performance by mitigating the vulnerabilities and defend well in the presence of selective drop attack.

III. HYPOTHETICALSOLUTION FOR RSDA USING ECDSA

The malicious nodes have to be detected; otherwise there are loopholes for overloading a host and entirely stopping it from working [41]. Thus, the node which denies forwarding certain messages, but sending other messages to act unpredictably should be identified.

A. EFFECT OF MALICIOUS NODE OR COMPROMISED NODE

If there are one or more malicious nodes of node s in the neighborhood and the node n_2 is a gray hole node, which is not similar to the selfish node, these nodes will selectively or randomly drop data packets [16]. This is harmful to data traffic. Suppose s has n_2 as the next hop and if s is not able to communicate with nodes which are k-hop away, then it is assumed that all the nodes are gray hole nodes. Hence the node s has to be isolated from the malicious neighbors.

A compromised node in MANET [23] is a node, in which the attackers obtain the control through unfair with the aim of carrying out malicious activities. The nodes in MANET are independent in nature, and the nodes cannot prevent the malicious activities to which they are communicating. Since the compromised node changes its position very frequently and the nodes can join and leave the network irrespective of time and place, hence it becomes tough to track or monitor the malicious activities. Based on the analysis, node misbehavior and gray hole attack make node isolation process a more complicated task, and it may affect the connectivity of every node.

Based on the investigation of node isolation process, it is observed that if the node does have any gray hole node, then the node must be isolated from the network. To facilitate the node isolation problem, it is necessary to define the possible paths for a node. For a pair of nodes (s, d), if the path between them is not less than two, i.e., *s* and *d* are at least two hops away, or k-hops away, then all paths existing between *s* and *d* are known as out-going (s, d)-paths for *s* or *d*. Some outgoing paths are available to enable a node for communicating with other nodes beyond its range. When node *s* has selfish node connectivity, it can be isolated by its neighboring nodes.

To define the outgoing path, the degree is determined as $D_c(s)$, of node s as the maximum number of outgoing paths of s. Let $n_i(s)$ be the number of node s's neighbor at the state i ($i \in S$) and $n_g(s)$ the number of s's gray hole neighbors, respectively. A node communicates with the other nodes via k outgoing links. Thus k-connectivity of individual nodes could be determined. The node *s* is assumed with degree *d*, D(s)=d, u is said to be k-connected if its cooperative node's degree is k, $D_c(s)=k$, if s has no gray hole neighbor and k cooperative neighbors, $n_g(s)=0$ and NC(s)=k respectively.

In selective drop attack, the malicious nodes would refuse of forwarding message passing through them. At last this attack can potentially drop the throughput of a host to a minimum level. The RSDA protocol has been proposed to strengthen the resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing by disabling the link as defective or attempts to obtain a new efficient route to the destination. RSDA provides an effective security for selective drop attack. The attacker nodes can potentially drop the throughput of a host to the minimum level, and those nodes have been detected based on the elliptic curve digital signature algorithm (ECDSA) procedure.

B. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Elliptic curves are defined over finite algebraic structures such as finite fields o^n, where p is the prime integer and n the positive integer. Elliptic curve algorithms use smaller key sizes compared to other asymmetric cryptographic algorithms; hence processing speed can be increased.

As inferred from table 1, for the128-bit symmetric key to obtain an equivalent strength of security with an asymmetric algorithm, it is necessary to choose 3072-bit size key. However, the equivalent key length is 256 with elliptic curve algorithms. It offers equivalent security as asymmetric cryptographic algorithms but with shorter key size. The performance is improved with lesser storage power and bandwidth requirements.

TABLE 1. Key length comparison.

Symmetric technique Key length	Asymmetric technique Key length	Elliptic curve key length
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

The elliptic curve can be defined in the form of the equation,

$$Y^2 = x^3 + ax + b \pmod{p} \tag{1}$$

where x, y, a, b ∈ **R**. and R is the region.

To define a curve, the factors such as name and domain parameters set which comprise of *p, n, a, b, x, y* of base point g(x,y) on the curve are required. The elements in domain parameter set are taken as *p* prime modulus, *n* prime order, *a, b* coefficients, and *x, y* coordinates. For the computation of ECDSA, a pair of keys (private key, public key) is generated; signature should be created and verified with the generated private and public keys.

C. KEY GENERATION

The procedure for generating pair of keys are given as follows,

The private key *d* (a numeric value) is generated from pseudo-random number known as a nonce,and the public key can be obtained from the private key and the elliptic curve domain parameters.

In Algorithm 1, assume if user "A" requests to send a signed message to user "B". Primarily, they must agree on the curve limits (CURVE, G, n). In addition to the field and equation of the curve, it needs G, a base point of major order on the curve; *n* is the multiplicative order of the point G. The alternative method ECDSA signature might escape private keys when *k* is produced by a defective accidental number generator.. Such a failure in random number generation caused users of Android Bitcoin Wallet to lose their funds in August 2013.

The key and signature-size comparison of elliptic-curve cryptography to DSA in general, the bit size of the public key supposed to be desired for ECDSA is about double the scope of the security level, in bits.

The public key $q(x, y)$ can be computed by performing point multiplication with the base point g(x, y). It is given

Algorithm 1 Key Generation

```
Output: Apply ECDSA Key generated
Input: Input value read enduring process a generate key
1.  Begin
2.  Generate Random Number (nonce) k
3.  Form Private Key d
4.  Compute e=HASH(m), // HASH is cryptographic hash function
5.  Let z be the $L_n$ leftmost bits of e, where $L_n$ is the bit length of the group order n.
6.  Choice a Cryptographically Secure Random (CSR) integer k from [1, n−1].
7.  Compute the curve point (x, y)=k×G.
8.  Compute r=x mod n If r=0, go back to step 3.
9.  Compute s= $k^{-1}(z =rd_A)$ mod n. If s=0, go to step Select CSR.
10. Signature is the pair (r,s).
11. Finally, form a Public Key Q (x, y)
12. End
```

as follows,

$$q(x, y) = d * g(x, y) \tag{2}$$

Finding accuracy of an algorithm for how efficiently computing all the verification approach is not directly clear. To see why, mean as S the curve point is calculated in step 9 of verification [24]

$$S = a \times G + b \times Q_x \tag{3}$$

From the classification of the public key as $Q_x = d_x \times G$

$$S = a \times G + bd_X \times G \tag{4}$$

Because elliptic curve scalar multiplication distributes over addition,

$$S = (a + b)d_X \times G \tag{5}$$

Growing the definition of a and b from verification step 8,

$$S = (zp^{-1} + rd_X p^{-1}) \times G \tag{6}$$

Gathering the common term p^{-1}

$$S = (z + rd_X)p^{-1} \times G \tag{7}$$

Expanding the definition of s from signature step 9

$$S = (z + rd_X)\,(z + rd_X)^{-1}\left(k^{-1}\right)^{-1} \times G \tag{8}$$

Since the inverse of an inverse is the original element, and the product of an element's inverse and the element is the identity, left with

$$S = k \times G \tag{9}$$

From the definition of r, this is verification step 9.

The private key is known only to the sender node, and the public key is openly accessible. The private key is generated from nonce, and thepublic key is generated based on ECDSA key generation algorithm, figure 3 illustrates how the pair of keys can be generated. The domain parameters such as *p, n, a, b, x, y* are essential in ECDSA key generation algorithm for generating the public key.

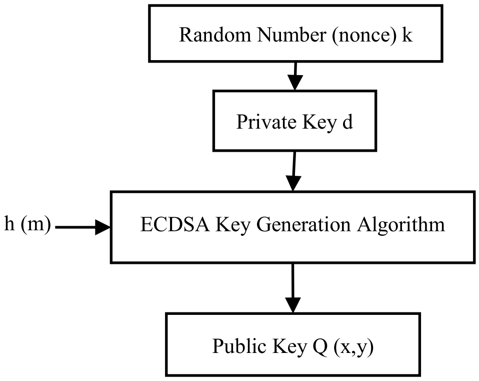

FIGURE 3. ECDSA Key generation process.

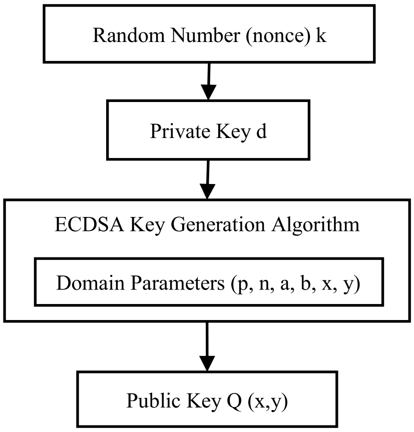
Random Number (nonce) k
Private Key d
ECDSA Key Generation Algorithm
Domain Parameters (p, n, a, b, x, y)
Public Key Q (x,y)

FIGURE 4. ECDSA signature creation process.

D. SIGNATURE CREATION

Using authenticated public key, the recipient can verify the received message. The variable length message is changed as fixed length message digest h(m) using SHA-2 [25].

It is not feasible to computationally derive the message from the received message digest. If the message is modified, it reflects a significant change in the message digest. Figure 4 shows how the signature is created.

ECDSA signature creation algorithm is described below,

In the digital signature, *r* and *s* are two integer values. The value for *r* is computed using the random number *k* and the base point g(x, y).

$$(x1, y1) = k * g(x, y) \bmod p \tag{10}$$

$$R = x_1 \bmod n \tag{11}$$

If the value of *r* iszero, a new random number *k* must be chosen,and then *r* should be computed again.

Algorithm 2 Signature Verification

```
Input: For Y to authenticate X signature, the user must have a copy of her public-key curve point $Q_x$.
Output: X can verify $Q_x$ is a valid curve point for successfully sending.
Process
1. Begin
2. Created message can be sent Y for verification using authenticator's public key
3. The message digest is intended with the public keyq(x, y)
4. Digital signature elements r and s
5. Check that $Q_x$ is not equal to the identity element $O$, and its coordinates are otherwise valid
6. Y to authenticate X signature
7. Check that $Q_x$ lies on the curve
8. X can verify $Q_x$ is a valid curve point for successfully sending
9. All verification elements with domain Parameters (p, n, a, b, x, y)
10. Check that $n \times Q_x = \mathrm{O}$
11. Consecutive secure Public key with different curve points
12. End
```

To obtain the value of s, assign the input as message digest h(m); the random number as k and the private key as d. It can be calculated as,

$$\mathrm{S} = (\mathrm{k}^{-1}(\mathrm{h(m)} + \mathrm{d} * \mathrm{r}) \bmod \mathrm{n} \tag{12}$$

's' must not be zero to be a valid number. If the value of s is obtained as zero, a fresh random number k must be chosen and then re-computed. Ineq. 12

On the receiver side, once the message (r, s) is computed, and the value of k is provided for elliptic curve computations.

E. SIGNATURE VERIFICATION

The received message can be verified using authenticator's public key, and the message is calculated with the public key q(x, y), and the digital signature elements r and s. Figure 5 depicts the process of signature verification [26], For verifying the signature, the inputs needed are h(m), q(x, y), r, s and g(x, y). ECDSA signature verification algorithm2 is described as the signature verifying process for X sending a message to Y with signature towards "Y" verification public key.

The verification of the generated signature, the inputs needed are h(m), q(x, y), r, s, and g(x, y). ECDSA signature verification is defined, Process for X Sending a message with the public key to Y with signature towards "Y" encrypted the key. It is not closely understandable why verification even functions correctly. In the process of signature verification algorithm 3,verifies the signature, once message with Public Key Y follows the Message received with a security key to Receiver "Y". Computed Message Public Key successfully ready to declare that the signature is valid if r=x(mod n), invalid otherwise. It displays that to validate "Y", many other properties are essential for a secure signature algorithm.

Algorithm 3 Validating Signature

```
Input: Message received with security key to Receiver "Y"
Output: Computed Message Public Key successfully ready
Process
1. Begin
2. Verify that and $r$ ares integers in $[1, n - 1]$. If not, the signature is invalid.
3. Calculate e=HASH(m), // HASH is the same function used in the signature generation.
4. Digital Signature (r, s)
5. Let z be the $\mathrm{L_n}$ leftmost bits of e
6. Calculate $w = sww = s^{-1} modn$
7. Calculate $w = swu_1 = zwmodnandu_2 = rwmodn$
8. Calculate the curve point $(x, y) = u_1 \times G + u_2 \times Q_x$. If $(x, y)((x, y) = O$ then the signature is invalid.
9. The signature is valid if $r = x(modn)$, invalid otherwise.
10. End
```

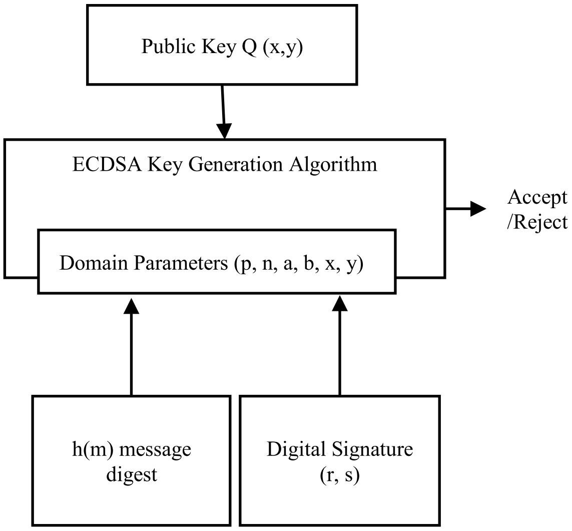

FIGURE 5. ECDSA signature verification process.

$$\mathrm{W} = \mathrm{s}^{-1} \bmod \mathrm{n} \tag{13}$$

$$\mathrm{P1} = (\mathrm{h(m)} * \mathrm{w}) \bmod \mathrm{n} \tag{14}$$

$$\mathrm{P2} = (\mathrm{r} * \mathrm{w}) \bmod \mathrm{n} \tag{15}$$

$$(\mathrm{x2}, \mathrm{y2}) = (\mathrm{p1} * \mathrm{g(x, y)} + \mathrm{p2} * \mathrm{q(x, y)}) \bmod \mathrm{n} \tag{16}$$

If the value of x2 is equivalent to r, then the signature verification is successful, and the received message can be accepted. Otherwise, it would be rejected if the value of x_2 doesnot match with r.

1. The protocol has less routing overhead since it is using ECDSA with less key size but with same security level.

It discourages and defends against selective drop attack by selecting the active route which is not attacked before. In RSDA protocol, the sender generates a key pair – private key d and public key $q(x, y)$. The public key $q(x, y)$ can be created by using private key d, elliptic curve domain parameters (p, n, a, b, x, y) along with the base point $g(x, y)$ on the curve. The digital signature r and s are sent to the respective destinations by the sender after the completion of signature creation. The destination node completes this verification with the communicated public key. Each intermediate node examines the verification of the source node by receiving the RREQ packet. ECDSA based authentication code is used for the reliability of the RREQ packet. AODV [27] routing protocol is taken as the base protocol and modified according to the proposed protocol.

IV. EXPERIMENTAL SETUP

The experimental setup implements RSDA on a real system and evaluates the performance of the protocol. The RSDA protocol was implemented on three laptops (with Intel i7 processors) running the Red Hat Linux operating systems (version 7.4). We compared the performance of two RSDA implementations by UCSB [28] and UU [29]. Simulations were conducted on static and dynamic scenarios to evaluate the performance of RSDA.

The NETPIPE [30] software sends packets with increasing size and provides us with the following information: time taken to transfer the block, throughput in bits/sec, number of bits in the block transferred, and number of bytes in the block transferred. The knowledge behind the collection of packet size is to compare and measure the throughput for various packet sizes. Ideally, for small packet size, the throughput is less and with increasing packet size, it increases until a point after which it saturates.

For the static scenario, the experiment was conducted for various packet sizes and the throughput graph, network signature graph, and saturation graph were plotted using the above information provided by the software. For the dynamic scenario, the source code of the software was modified so that the packets size does not increase and hence the experiment was conducted for fixed packet sizes.

A. DETECTION OF SELECTIVE DROP ATTACK

The transmission rate tr is broadcasted periodically by the source in an Authenticated Route Request (AREQ) packet after signing it. Then, the nodes add their estimated transmission rate to the packet upon receiving it and store the latest copy of AREQ. The selective drop attack performed by the downstream nodes can be detected by AREQ packet, as shown in figure 6.

If the transmission rate is increased or decreased extensively, then the data transmission advances towards the destination, each node checks the weight of the link. If the variation between the last rate in AREQ and the node's estimated value is greater than the threshold value, then it is proven that at least one malicious node exists between nodes and the node is the one which added its last rate to AREQ. If the node notices an extreme variance, then the link will be disjointed from its parent as defective or malicious and takes up the responsibility for searching a new route to the destination.

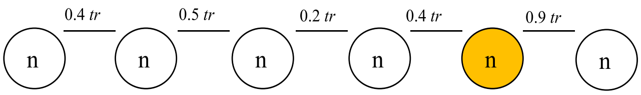

FIGURE 6. Selective drop attack.

ECDSA [24] based authentication has been used for preventing the modification of RREQ and RREP messages. The modified format of RREQ and RREP packet frames are shown below.

Modified messages for RREQ packet frame as follow:

<table>
<tr><td>Type</td><td>D</td><td>G</td><td>Reserved</td><td>Hop count</td></tr>
<tr><td colspan="5">RREQ ID</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Destination sequence number</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Source sequence number</td></tr>
</table>

Modified messages for RREPPacket frame as follow:

<table>
<tr><td>Type</td><td>A</td><td>Reserved</td><td>Hop count</td></tr>
<tr><td colspan="4">RREQ ID</td></tr>
<tr><td colspan="4">Destination IP Address</td></tr>
<tr><td colspan="4">Destination sequence number</td></tr>
<tr><td colspan="4">Source IP Address</td></tr>
<tr><td colspan="4">Source sequence number</td></tr>
</table>

The reserved bits in RREQ and RREP packets are used for analyzing the total number of packets sent by the source node,and the destination node verifies the same. AREQ and Authenticated Route Reply (AREP)[31] packets are used for checking the transmission rate. ECDSA based authentication code is attached with the message to mitigate from tampering of messages. In RSDA, AREQ is appended with the RREQ packet to accumulate the transmission rate value. The selective drop attack can be identified by checking the difference of a node with 2-hop neighbors and the nodes threshold value.

B. ROUTE DISCOVERY PROCESS

In RSDA protocol, if a node s wants to send a packet to a destination node d, it initiates the route discovery process by sending a route request RREQ packet. In addition to the signed AREQ, it contains the source and destination ids and a request *id*, which is generated randomly and an ECDSA

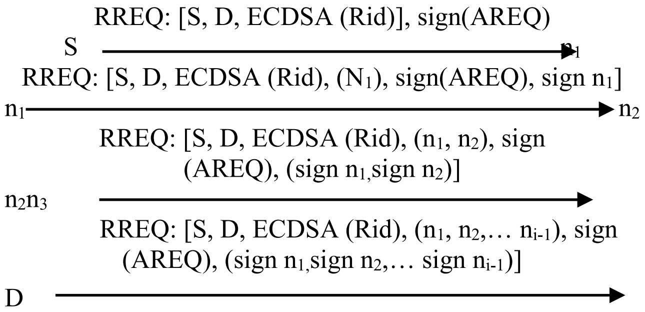
RREQ: [S, D, ECDSA (Rid)], sign(AREQ)
S
n1
RREQ: [S, D, ECDSA (Rid), (N1), sign(AREQ), sign n1]
n1
n2
RREQ: [S, D, ECDSA (Rid), (n1, n2), sign (AREQ), (sign n1,sign n2)]
n2n3
RREQ: [S, D, ECDSA (Rid), (n1, n2,… ni-1), sign (AREQ), (sign n1,sign n2,… sign ni-1)]
D

FIGURE 7. ECDSA based route request.

is computed over the request id with a key shared by the sender and the destination. If an intermediate node receives the RREQ packet for the first time, the node adds its id to the maintained list of node ids and signs it with a key which is shared with the destination. It then forwards the RREQ to its neighbors as shown in figure 7.

Let n_1, $n_2 \ldots n_{i-1}$ be the set of nodes that takes place between the source S and the destination D.If the destination node receives the gathered RREQ message, it first verifies the sender's request id by computing the signature with the sender's public key.

It then checks the digital signature of all intermediate nodes. Once all the verifications are successful, the destination node then initiates the route reply process by generating the RREP message otherwise RREQ packets would be discarded by the destination node. It again constructs a signature by ECDSA procedure on the request id with the key shared by the sender and the destination. The RREP packet contains the id's of both the source node and the destination node, the ECDSA of the request id, the accumulated route from the RREQ packet which is digitally signed by the destination. The RREP packet is sent back the source node along the reverse route.

C. ROUTE REPLY PROCESS

If the intermediate node receives the RREP packet the reverse process occurs; it verifies whether it's id is in the list of ids stored by the RREP. It also verifies the ids of all its neighbors in the list. The intermediate node then checks whether the digital signature of the destination node stored in the RREP packet is valid or not. If it is valid, then the RREP packet is accepted, or else it is dropped. The route reply process is illustrated in figure 8.

In RSDA protocol, authentication is performed for both RREQ and RREP operations. Only the nodes participating in the current route need to perform these cryptographic computations thus making the proposed protocol more efficient and secure. The protocol achieves better delivery ratio with reduced overhead and jitter with minimal use of node energy by detecting selective drop attacks when compared to the base mechanism.

When the source node receives the RREP packet, it first checks if the first id of the route stored by the RREP is its adjacent node. If so, then it verifies all the digital signatures of the intermediate nodes in the RREP packet. Once all these verifications are successful, then the source node agrees on the route for data transmission. The source also checks the request id that is sent along with RREQ packet. If the source node receives the same request id back from the destination, then it decides that there is no replay attack.

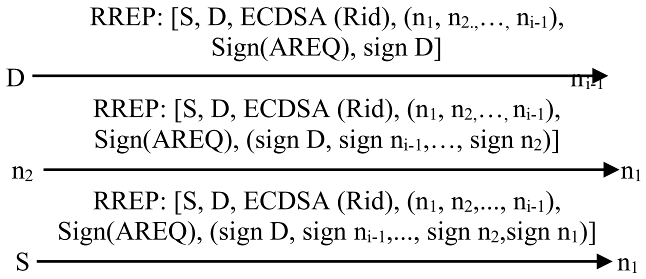
RREP: [S, D, ECDSA (Rid), (n1, n2.,…, ni-1), Sign(AREQ), sign D]
D
ni-1
RREP: [S, D, ECDSA (Rid), (n1, n2,…, ni-1), Sign(AREQ), (sign D, sign ni-1,…, sign n2)]
n2
n1
RREP: [S, D, ECDSA (Rid), (n1, n2,..., ni-1), Sign(AREQ), (sign D, sign ni-1,..., sign n2,sign n1)]
S
n1

FIGURE 8. ECDSA based route reply.

TABLE 2. Notations and description.

Notation	Description
X, Y	Two Users Act as Sender and Receiver
K	Random Number
Tr	Transmission Rate
Q_x	Quadratic Points
g(x, y)	Base Points
S	Source
D	Destination
CURVE	Elliptic curve field and equation used
G	Elliptic curve base point, a generator of the elliptic curve with large prime order n
N	Integer order of G means that nxG=0
(p, n, a, b, x, y)	Curve domain parameters
P	Packet
Q (x, y)	Public Key
D	Private Key
HASH	Function used for
L_n	Leftmost bits
(n_1, $n_{2,\ldots,}$ n_{i-1})	Nodes
(r, s)	Digital Signature
h(m)	Message summary

The problems in MANET [32] could be that the data transmission is not only with a single node; hence the single node may not support packet forwarding. This could happen insome scenarios where it has a high load, or when the node is a selfish one. There may not be proper CPU cycles, enough buffer space or available bandwidth to forward packets. Thismakes the MANET more vulnerable to expenses and breakdowns. Therefore, it becomes vital to detect the malicious nodes to improve the performance of MANET.

V. RESULTS AND DISCUSSION

The simulation has been conducted to validate the detection and isolation of the proposed scheme against gray hole nodes. In an area of 1000m × 1000m, 60 normal nodes executing the routing protocol were randomly distributed,and one or a couple of malicious nodes which is selectively dropping packets are randomly located. Ten pairs were randomly chosen for

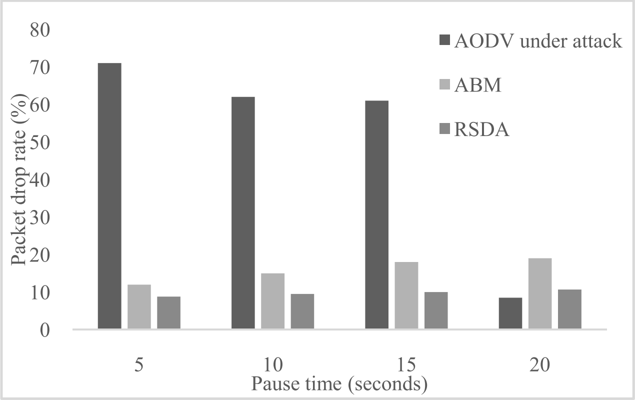

FIGURE 9. Packet drop rate *vs.* pause time.

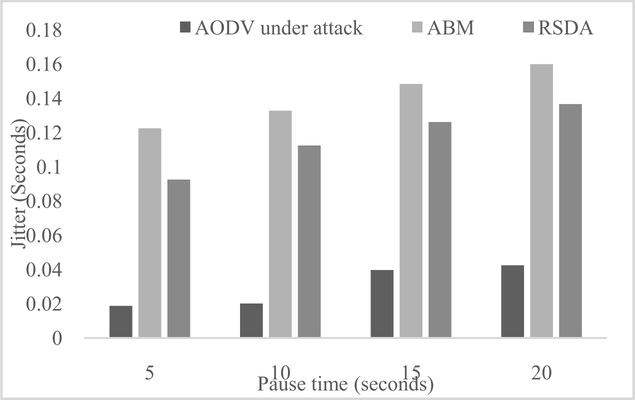

FIGURE 10. Jitter *vs* pause time.

data communication [10], [31], each sending 5 kb UDP-CBR per second. All normal nodes were moved based on RWM with random speeds ranging from 0 to 15 m/s. The pause time of nodes was considered as 5s, 10s, 15s, and 20s.

A. PACKET DROP RATE

The drop rate [33] was raised to about 63.9% when there were gray hole nodes randomly fixed at various positions at all pause time as 5, 10, 15,20seconds respectively. In the presence of gray hole nodes, the total packet drop rate of the approach achieved was16.7%. With the deployment of proposed RSDA, the drop rate successfully reduced to about 9.56% rate, as shown in figure 9. The packet drop rate [34] is shown to decrease significantly when more misbehaving nodes make abnormal routing operations. This effect is particularly severe to the network with more number of nodes.

B. JITTER

Jitter value raised to about 0.56% when there were gray hole nodes randomly fixed at various positions at all pause time as 5s, 10s, 15s, 20seconds respectively. As presented in figure 10, in the presence of gray hole nodes, the total delay of the approach achieved was 0.14%. With the deployment of proposed RSDA, the jitter rate was successfully reduced to about 0.115% rate.

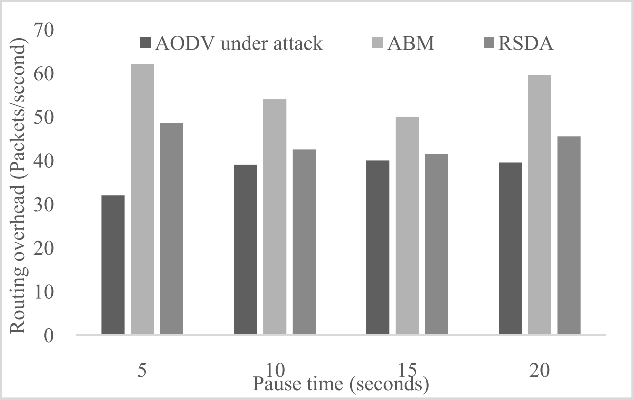

FIGURE 11. Routing overhead *vs.* pause time.

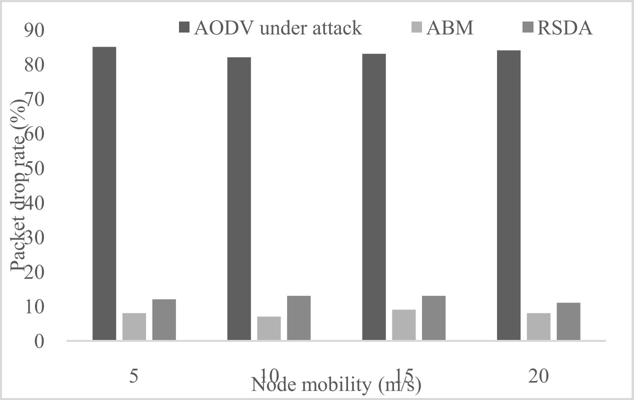

FIGURE 12. One gray hole node for node mobility *vs.* packet drop rate.

C. ROUTING OVERHEAD

The routing overhead was raised to about 77.84% when gray hole nodes were randomly fixed at various positions at all pause time as 5s, 10s, 15s, 20seconds respectively. In the presence of gray hole nodes, the routing overhead of the existing approach was56.85%. With the deployment of proposed RSDA, the routing overhead was successfully reduced to about 45.49% rate, as shown in figure 11.

D. PACKET DROP RATE FOR RANDOMLY MOVED GRAY HOLE NODES

In addition to 60 normal nodes distributed, 1 or 2 gray hole nodes in network topology are considered separately. First, it was assumed that gray hole nodes are randomly moved. The total packet drop rate of one gray hole node [26] and two gray hole nodes are as shown in figures 12 and 13 respectively and the total packet drop rate is depicted when the nodes are at different mobility speeds. Packet drop rate is also defined as the number of packets failed to reach the destination, to the number of packets transmitted from all source nodes in the network. The network might miss packets due to reasons such as congestion, mobility, traffic without gray hole nodes.

In the absence of gray hole nodes, the total packet drop rate for all mobility speed by AODV [27], [35]–[37] is about 7.93% with all nodes randomly moved. The drop rate raises

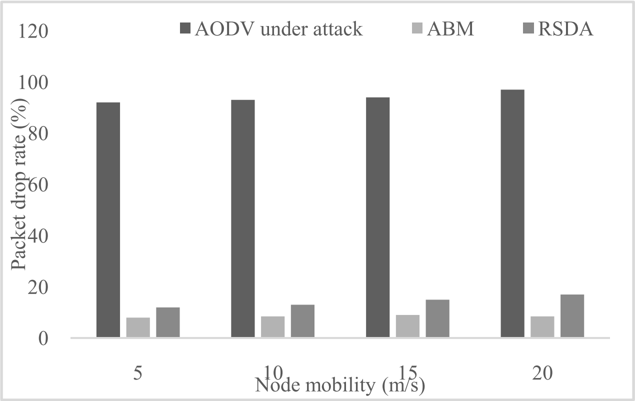

FIGURE 13. Two gray holes nodes for node mobility *vs.* packet drop rate.

to about 86.75% when there is one gray hole node randomly fixed at various positions. With the deployment of proposed RSDA, the drop rate can successfully reduce by about 12.63%. In the absence of two gray hole nodes, the total packet drop rate for all mobility speed by AODV is about 8.6% with all nodes randomly moved.

The drop rate is raised to about 94.89% when there are two grey hole [26], [38] nodes randomly fixed at various positions. With the deployment of the proposedRSDA, the drop rate can successfully have reduced by about 14.5%. An interesting observation is that the proposed method shortens the packet drop rate significantly, especially for the scalable network. In fact, it achieves the significant security level with less key size.

VI. CONCLUSION AND FUTURE WORK

Resistive to Selective Drop Attack (RSDA) attempts to provide an effective security for selective drop attack. It is important that the illegitimate nodes should be identified which overload a host and isolate them from the network by holding its transmission process. In selective drop attack, the neighboring nodes will not loyally forward their messages to the next node. However, a malicious node which has been entered itself in the data flow path can deny specific forwarding messages. The malicious nodes have to be detected, which is overloading a host and entirely stop it from working. Thus, the node which denies forwarding certain messages, but sending other messages acted unpredictably. In selective drop attack, the malicious nodes would be refusing of forwarding messages passing through them. At last the attack can potentially drop the throughput of a host to the minimum level. Security in a WANET environment requires a precise point of view, from which security can be provided by mitigating the protection against various types of attacks.

REFERENCES

[1] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," *Encycl. Telecommun.*, vol. 1, no. 1, pp. 1–28, Dec. 2002.

[2] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): Challenges and perspectives," in *Proc. 6th Int. Conf. Telecommun.*, 2006, pp. 761–766.

[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 70–75, Oct. 2002.

[4] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, 2005.

[5] V. Balakrishnan and V. Varadharajan, "Packet drop attack: A serious threat to operational mobile ad hoc networks," in *Proc. Int. Conf. Netw. Commun. Syst. (NCS)*, Krabi, Thailand, 2005, pp. 89–95.

[6] M. Peng, W. Shi, J.-P. Corriveau, R. Pazzi, and Y. Wang, "Black hole search in computer networks: State-of-the-art, challenges and future directions," *J. Parallel Distrib. Comput.*, vol. 88, pp. 1–15, Feb. 2016.

[7] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Syst. J.*, vol. 9, no. 1, pp. 65–75, Mar. 2015.

[8] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 103–112, Apr. 2015.

[9] P. Chen, S. Cheng, and K. Chen, "Information fusion to defend intentional attack in Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 337–348, Aug. 2014.

[10] X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," in *Proc. Amer. Control Conf. (ACC)*, vol. 1, 2013, pp. 3002–3007.

[11] F. Razzak, "Spamming the Internet of Things: A possibility and its probable solution," *Procedia Comput. Sci.*, vol. 10, pp. 658–665, Jan. 2012.

[12] J.-H. Cho, R. Chen, and K. S. Chan, "Trust threshold based public key management in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 44, pp. 58–75, Jul. 2016.

[13] J. Friginal, D. de Andrés, J.-C. Ruiz, and M. Martínez, "REFRAHN: A resilience evaluation framework for ad hoc routing protocols," *Comput. Netw.*, vol. 82, pp. 114–134, May 2015.

[14] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," *Ad hoc Netw.*, vol. 19, pp. 142–155, Aug. 2014.

[15] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2096–2114, 2013.

[16] D. Cheelu, M. R. Babu, and P. Venkatakrishna, "A fuzzy-based intelligent vertical handoff decision strategy with maximised user satisfaction for next generation communication networks," *Int. J. Process Manage. Benchmarking*, vol. 3, no. 4, pp. 420–440, Jan. 2013.

[17] R. V. Boppana and X. Su, "On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 8, pp. 1162–1174, Aug. 2011.

[18] Y. Yu, L. Guo, X. Wang, and C. Liu, "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks," *Comput. Netw.*, vol. 54, no. 9, pp. 1460–1469, Jun. 2010.

[19] A. Khan, T. Suzuki, M. Kobayashi, W. Takita, and K. Yamazaki, "Packet size based routing for stable data delivery in mobile ad-hoc networks," *IEICE Trans. Commun.*, vol. 91, no. 7, pp. 2244–2254, 2008.

[20] N. Komninos, D. Vergados, and C. Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 5, no. 3, pp. 289–298, 2007.

[21] A. K. Khare, J. L. Rana, and R. C. Jain, "Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 7, p. 29, 2017.

[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc Netw.*, vol. 1, no. 2, pp. 293–315, 2003.

[23] A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs," *Ad Hoc Netw.*, vol. 13, pp. 368–380, Feb. 2014.

[24] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[25] D. Zhong, H. Lv, J. Han, and Q. Wei, "A practical application combining wireless sensor networks and Internet of Things: Safety management system for tower crane groups," *Sensors*, vol. 14, no. 8, pp. 13794–13814, 2014.

[26] C. K. Doshi, S. Sankaranarayanan, V. B. Lakshman, and K. Chandrasekaran, "Game theoretic modeling of gray hole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Signal, Netw., Comput., Syst.*, 2017, pp. 217–226.

[27] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on-Demand Distance Vector (AODV) Routing*, document RFC 3561, Nokia Research Center, IETF, 2003

[28] Z. Kebir, M. Omari, and H. Soulimani, "Mobile adhoc network protocols simulation: Distance vector vs source routing comparison," *Wireless Netw.*, vol. 6, no. 2, pp. 25–34, 2017.

[29] R. N. Ode, D. Perdana, and R. F. Sari, "Performance evaluation of AODV, AODV-UU, and AODV with malicious attack mode on vehicular ad-hoc network," *Adv. Sci. Lett.*, vol. 23, no. 5, pp. 3990–3994, 2017.

[30] D. Eberius, T. Patinyasakdikul, and G. Bosilca, "Using software-based performance counters to expose low-level open MPI performance information," in *Proc. 24th Eur. MPI Users Group Meeting*, 2017, p. 7.

[31] H. U. Yildiz, K. Bicakci, B. Tavli, H. Gultekin, and D. Incebacak, "Maximizing wireless sensor network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies," *Ad Hoc Netw.*, vol. 37, pp. 301–323, Feb. 2015.

[32] H. Al Amri, M. Abolhasan, and T. Wysocki, "Scalability of MANET routing protocols for heterogeneous and homogenous networks," *Comput. Elect. Eng.*, vol. 36, no. 4, pp. 752–765, 2010.

[33] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and R. Magán-Carrión, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping," *Comput. Netw.*, vol. 87, pp. 44–58, Jul. 2015.

[34] A. Baadache and A. Belmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 1130–1139, 2012.

[35] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2471–2481, Jun. 2009.

[36] J. Von Mulert, I. Welch, and W. K. G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1249–1259, 2012.

[37] S. Krco and M. Dupcinov, "Improved neighbor detection algorithm for AODV routing protocol," *IEEE Commun. Lett.*, vol. 7, no. 12, pp. 584–586, Dec. 2003.

[38] P. Chawla and M. Sachdeva, "Detection of selective forwarding (Gray Hole) attack on LEACH in wireless sensor networks," in *Next-Generation Networks*. Singapore: Springer, 2018, pp. 389–398.

[39] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "A secure protocol for spontaneous wireless ad hoc networks creation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 629–641, Apr. 2013.

[40] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks," *J. Netw. Comput. Appl.*, vol. 34, no. 2, pp. 492–505, 2011.

[41] S. Khan and J. Lloret-Mauri, *Security for Multihop Wireless Networks*. Boca Raton, FL, USA: CRC Press, 2014.

[42] A. B. Bomgni, M. L. F. Sindjoung, A. B. Bomgni, E. T. Fute, G. Chalhoub, and C. T. Djamegni, "ISCP: An instantaneous and secure clustering protocol for wireless sensor networks," *Netw. Protocols Algorithms*, vol. 10, no. 1, pp. 65–82, 2018.

[43] A. Ranjan, V. Kuthadi, T. Marwala, and R. Selvaraj, "Swarm based architecture for defense against stealthy attacks in mobile ad hoc network," *Ad Hoc Sensor Wireless Netw.*, vol. 36, nos. 1–4, pp. 107–126, 2017.

T. POONGODI received the Ph.D. degree in information technology (information and communication engineering) from Anna University, Chennai, India, in 2017. She is currently an Associate Professor with the School of Computing Science and Engineering, Galgotias University, NCR Delhi, India. She has presented papers in national/international conferences; has published book chapters in CRC Press, IGI global, and Springer; and has edited books. Her main thrust research areas are big data, the Internet of Things (IoT), ad-hoc networks, network security, and cloud computing. She is a Pioneer Researcher in the areas of WSN and the IoT, and has published over 25 papers in various top international journals.

MOHAMMED S. KHAN received the M.Sc. and Ph.D. degrees in computer science and computer engineering from the University of Louisville, Louisville, KY, USA, in 2011 and 2013, respectively. He is currently an Assistant Professor of computing with East Tennessee State University, and also the Director of the Network Science and Analysis Lab. His primary area of research is in ad-hoc networks, network tomography, and connected vehicles. He currently serves as the Co-Editor-in-Chief for the *International Journal of Grid and High-Performance Computing*. He has been on the technical program committees of various international conferences. He has been a Technical Reviewer of various international journals in his field. He is a member of the IEEE.

RIZWAN PATAN received the B.Tech. and M.Tech. degrees from Jawaharlal Nehru Technological University Anantapur, India, in 2012 and 2014, respectively, and the Ph.D. (computer science and engineering) degree from the School of Computer Science and Engineering, VIT University, Vellore, India, in 2017. He is currently an Assistant Professor with the School of Computing Science and Engineering, Galgotias University, NCR Delhi, India. He has published reputed eight SCI journals and 20 free Scopus indexed journals. He has also presented papers in national/international conferences; has published book chapters in CRC Press, IGI global, and Elsevier; and has edited books. He holds two Indian patents. He is a Guest Editor of the *International Journal of Grid and Utility Computing* (Inderscience), and the *Recent Patents on Computer Science, Information Medical Unlock* (Elsevier).

AMIR H. GANDOMI received the Ph.D. degree in engineering. He used to be a Lecturer in several universities. He is currently an Assistant Professor of analytics and information systems with the School of Business, Stevens Institute of Technology. Prior to joining Stevens, he was a distinguished Research Fellow with the headquarters of BEACON NSF Center, Michigan State University. He has published over 130 journal papers and four books. Currently, some of those publications are among the hottest papers in the field, and have been collectively cited over 8,500 times (h-index = 47). His research interests are global optimization and (big) data mining using machine learning and evolutionary computations in particular. He has also served as an Associate Editor, Editor, and Guest Editor for several prestigious journals, and has delivered several keynote/invited talks. He is a part of the NASA technology cluster on big data, artificial intelligence, and machine learning. Recently, he has been named as the 2017 Highly Cited Researcher (top 1%) and one of the world's most influential minds. He is currently ranked 20th in GP bibliography among over 10,000 researchers.

BALAMURUGAN BALUSAMY is currently a Professor with the School of Computing Science and Engineering, Galgotias University, NCR Delhi, India. He has published more than 70 papers in various top international journals. His main thrust research areas are big data, network security, and cloud computing. He is Pioneer Researcher in the areas of big data and the IoT.