electronics

MDPI

Article

A Novel Anomaly Behavior Detection Scheme for Mobile Ad Hoc Networks

Neeraj Chugh [1,2], Geetam Singh Tomar [3], Robin Singh Bhadoria [4] and Neetesh Saxena [5,*]

[1] Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies Dehradun, Dehradun 248001, Uttarakhand, India; nchugh@ddn.upes.ac.in
[2] Faculty of Computer Science & Engineering, Uttarakhand Technical University, Dehradun 248001, Uttarakhand, India
[3] Rajkiya Engineering College (REC), Sonbhadra 231206, Uttar Pradesh, India; gstomar@ieee.org
[4] Department of Computer Science & Engineering, Birla Institute of Applied Sciences (BIAS) Bhimtal, Nainital 263136, Uttarakhand, India; robin19@ieee.org
[5] School of Computer Science and Informatics, Cardiff University, Cardiff CF24 3AA, UK
* Correspondence: nsaxena@ieee.org

Abstract: To sustain the security services in a Mobile Ad Hoc Networks (MANET), applications in terms of confidentially, authentication, integrity, authorization, key management, and abnormal behavior detection/anomaly detection are significant. The implementation of a sophisticated security mechanism requires a large number of network resources that degrade network performance. In addition, routing protocols designed for MANETs should be energy efficient in order to maximize network performance. In line with this view, this work proposes a new hybrid method called the data-driven zone-based routing protocol (DD-ZRP) for resource-constrained MANETs that incorporate anomaly detection schemes for security and energy awareness using Network Simulator 3. Most of the existing schemes use constant threshold values, which leads to false positive issues in the network. DD-ZRP uses a dynamic threshold to detect anomalies in MANETs. The simulation results show an improved detection ratio and performance for DD-ZRP over existing schemes; the method is substantially better than the prevailing protocols with respect to anomaly detection for security enhancement, energy efficiency, and optimization of available resources.

Keywords: Mobile Ad Hoc Networks (MANETs); anomaly detection; anomaly behavior detection; security; energy preservation

check for updates

Citation: Chugh, N.; Tomar, G.S.; Bhadoria, R.S.; Saxena, N. A Novel Anomaly Behavior Detection Scheme for Mobile Ad Hoc Networks. *Electronics* **2021**, *10*, 1635. https://doi.org/10.3390/electronics10141635

Academic Editor: Huy Kang Kim

Received: 4 June 2021
Accepted: 5 July 2021
Published: 9 July 2021

1. Introduction

Mobile Ad Hoc Networks (MANETs) are prospective communication systems for all devices. Unlike wired infrastructure networks, MANETs functionalities are independent of sophisticated architecture, i.e., they are infrastructure-less and decentralized. In addition to the infrastructure-less and decentralized characteristics of MANETs, the dynamic nature of nodes poses diverse research issues associated with security, quality of service (QoS), anomaly/outlier/abnormal behavior detection, and clustering, etc. QoS is the most challenging job for developers due to continuous variation in the topology of MANETs. To attain a certain QoS, and sustain it, is difficult when the settings of the network frequently change. Moreover, because of multi hop routing in MANETs, each node is a router that enables information sharing by forwarding packets to other nodes. Hence, the default route is unavailable, and the solution to routing issues is complicated as there is seamless connectivity to other devices in its zone.

Maintaining security in the wireless link is difficult as it is more vulnerable when compared to a wired link. Since the first encryption was carried out, issues such as eavesdropping, encryption cracking, etc. have increased along with the user's input of spurious information, extended timeouts, and updates for the old routing table. There are several unresolved issues concerning security that require significant solutions for secure communication in ad hoc networks.

In traditional wired networks, the nodes are static; however, MANETs are capable of connecting any devices at a particular time in the network to communicate with one another. Researchers tend to focus on novel communication methods, i.e., wireless technology for data transmission, in which nodes are unrestricted in movement in the network; this is a restraint in wired networks. MANETs are widely employed in many applications due to the ease with which nodes can travel without restrictions and set up at a fast rate in such a network. Hence, MANETs have been used to establish a large set of applications. The nodes in the network communicate with one another by forwarding packets, consuming battery energy due to multi hopping in routes, and for transmission/reception of nodes in the network. The energy used by nodes i.e., battery power—means limited bandwidth and limited range of transmission; these are the most important concerns related to MANETs.

To construct and manage MANETs that are secure, efficient, and lightweight, mechanisms that involve reduced hardware resources are required; however, there is a lack of resources. Additional challenges include limited bandwidth, small subnets, traffic overhead, and high processing costs. The security primitives of confidentiality, authentication, authorization availability, and integrity need to work together for resource-constrained mobile devices. In the present study, resource-constrained key management networks are observed for the detection of outliers, and in addition, a lightweight key management network is built to ensure the stated security primitives through outlier detection. Also, we extend Teo and Tan's model [1] by incorporating outlier detection methods to build a secure key management network. Teo and Tan [1] proposed a method for key management in hierarchical MANETs that lacks energy efficiency due to the escalation of key messages because of dynamic topology and distant nodes that are considered to be constituents of a cluster in the hierarchy. Moreover, they have not considered the traits of network and routing security in their entirety. Another methodology, proposed by Traag et al. [2], is centered on a social event using the Bayesian location interference framework to enable the detection of nodes in the event; they also propose a scheme of event detection in their imminent activities. Nevertheless, this approach does not include performance parameters when sensing futuristic activities. One more significant work in the same field was carried out by Cerpa et al. [3], who proposed a data collection system architecture incorporating different filters to detect outliers. For the verification of outcomes, the Habitat monitoring dataset was, used and the authors assert that the proposed method is efficient for outlier detection; however, the study does not reflect the performance issues of the network.

The major contributions of this paper are to design solutions that address the challenges, along with the approaches that are highlighted in the background literature. This paper also integrates the protocol that proposes an improved, data-driven hybrid approach based on widely accepted protocols that are superior in energy efficiency, security, and the optimization of available resources. In addition, security in the wireless link is maintained, with more vulnerabilities tackled compared to a wired link. The proposed technique namely, the data-driven zone-based routing protocol (DD-ZRP) helps in the detection of outliers and energy-efficient cluster head selection for fault-tolerant routing in MANETs placed on data collected at both the network and subgroup levels. The novelty of this work is (1) to develop techniques based on flexible outlier definition for fault-tolerant routing in MANETs, (2) to calculate the in-network outcome to decrease both bandwidth and energy usage, (3) and to make dynamic updates to the data-driven hybrid approach. The findings reveal that the algorithm converges to a precise result, with justified communication load and energy consumption.

In MANETs, devices communicate without any pre-existing infrastructure, and these devices are generally mobile. To investigate MANETs, either software-based simulators or experimentation networks are used. The experimentation testbeds are chosen when the implementation involves some features of MANETs to be incorporated as radio propagation or energy consumption, which is fundamentally difficult to model precisely in simulators [4]. The real-world implementation of MANETs requires more effort, involves huge costs, and lacks flexibility; hence, most researchers favor simulators when compared to testbeds [5]. This becomes an impediment when the experimentation network size grows; the software-based simulation then becomes a feasible alternate and is an extensively used solution. Thus, considering the stated pros and cons of each approach, software-based simulations are used to preclude the huge efforts and costs required for real-life implementation. On the other hand, the simulations each time involve certain assumptions about the real world; these may turn out to be too coarse to include all facets that influence the performance of algorithms and protocols, so the simulation results have to be tested in the real-world environment for which they are designed. In the present work, software simulation is used to test the proposed DD-ZRP.

The remainder of the paper is arranged as follows: Section 2 covers the background and related work for outlier detection and energy preservation in MANETs; Section 3 discusses the proposed methodology for the detection of outliers and energy preservation in MANETs; Section 4 presents the results and discussion of the proposed approach in various protocols used for routing in MANETs; Section 5 presents the discussion and conclusion.

2. Background

Routing is the means of interchanging data between nodes in a network. Many routing protocols that are used for packet transfer have been proposed for MANETs; they differ from one another with respect to mechanism and performance. This is important in order to increase the network performance appropriately. This section presents a discussion of the performance and mechanism of the routing protocols considered in the present work, along with the security issues in MANETs.

2.1. *Ad Hoc On-Demand Distance Vector (AODV)*

AODV follows a hop-to-hop routing methodology and belongs to the category of reactive protocols. In AODV, the node issues route requests (RREQs) if there is a requirement to identify the route for a specific target node. The transitional/intermediary nodes forward the RREQs; a reverse route is also generated for the target node [6]. When the target node gets the route to the destination request, it creates a route reply (RREP) that comprises multiple hops needed to reach the target, as shown in Figure 1.

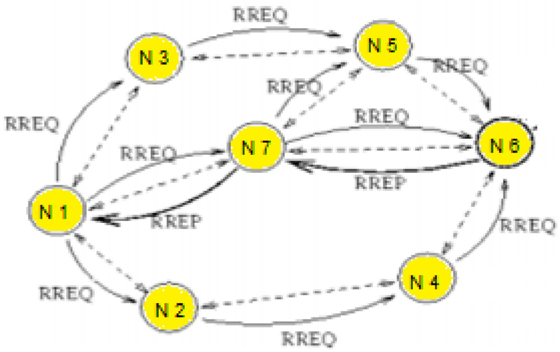

Figure 1. RREQ and RREP in AODV [7].

In AODV, the connection setup delay is less, as there is on-demand routing; to find the latest routes, sequence numbers are used [5]. However, AODV can have multiple route reply packets generated in reply to a particular route request packet, which may result in heavy control overhead.

2.2. *Dynamic Source Routing (DSR)*

Dynamic source routing is an on-demand/reactive protocol. In DSR, the route information is stored in the header packet, which travels from source to destination. To discover the path, the header packet is broadcast to all nodes, and in response, the destination sends the reply. The route between source and destination is established with the intermediary nodes when required; this results in a reduction of overhead and collision. The route request (RREQ) and route reply (RREP) primitives are employed to establish the path from source to destination. There can be multiple paths established; however, the final path setup is based on the least hop count. Thus, to keep track of the latest route, the routing table has to be updated regularly, along with the information in the header packet. This involves more energy consumption and causes node mobility delays in the larger networks.

2.3. Destination-Sequenced Distance Vector (DSDV)

DSDV is a proactive protocol [8] that involves multiple hops to reach the target node. This protocol uses routing tables located on every node for the transmission of data packets in the network. The presence of a routing table facilitates the reduction of high routing overhead and avoids loops [6]. DSDV is particularly suitable for creating a network with a lesser number of nodes; it requires a consistent update of the routing tables, which involves battery power usage and bandwidth.

2.4. Optimized Link-State Routing (OLSR) Protocol

The optimized link-state routing protocol (OLSR) is a proactive protocol that recurrently contacts other network nodes and shares topology information. The set of neighboring nodes chosen by the node are called multipoint relays (MPRs). The MPRs forward the control information anticipated for dispersal in the whole network; this facilitates a decrease in the required transmissions. MPR nodes provide the link-state information and are used to create the route between the source and destination nodes. OLSR makes the shortest path routes available for all destinations using the link-state information issued by MPRs. MPRs are selected by nodes amongst their one-hop neighbors, establishing bidirectional links; this helps in overcoming the issues of unidirectional links related to the transfer of data packets. The OLSR design facilitates how to work autonomously from other protocols, and makes no assumptions related to the underlying link layer.

2.5. Zone-Based Routing Protocol (ZRP)

The ZRP is a hybrid protocol that offers the merits of both reactive and proactive schemes. It distributes the network into flexible size zones. The zone size is dependent on the radius of length ρ, where ρ is the number of hops to the perimeter of the zone and not the physical distance. The communication between the nodes commonly takes place in close proximity, i.e., within the zone. Hence, finding out the routing information is easy with ZRP, showing the benefits of proactive protocols termed interzone routing protocols (IERPs). To find the route between the zones, an intrazone routing protocol (IARP) is employed, i.e., a reactive protocol [9]. At the time of communication, when one node requests to send a packet to another node, it checks for the availability of a destination within the zone; if it is present, then it casts the route request to border nodes that, in turn, check the availability in their zones. This continues until the search for a destination ends. On the other hand, as the routing zones greatly intersect, a node may belong to more than one routing zone. The problems to be resolved arise when a node receives the same query multiple times. Sinha et al. [10] describe how to resolve some of these problems and to overcome the traffic.

2.6. Security Issues in MANETs

The security issues and design of routing protocols in MANETs are dependent on different parameters such as origin, environment, range, QoS, and security criticality. The implementation of security varies if the range of networks differs. If the nodes are distant from one another, the threat of security attacks increases. Security issues are always perilous and need to be addressed in different routing protocols for MANETs.

In MANET routing protocols, nodes also act as routers and, thus, are involved in the exchange of information related to network topology. This is a significant flaw, because a compromised node may transmit information that is not updated to transmit traffic, or merely halt it. In addition, the routing protocols are extremely vulnerable in terms of security. The causes of the problems with MANET routing protocols include (1) the dynamic topology of ad hoc networks, (2) the infrastructure of ad hoc networks, (3) issues related to wireless communication viz. reduced security against signal and noise interference in wireless channels, and (4) the implicit trust relationship between neighbors.

Varieties of security mechanisms are designed and developed to avert malicious attacks. The classical methods viz. digital signature, encryption, authentication, and access control offer the first line of defense. As a second line of defense, cooperation enforcement mechanisms and intrusion detection systems are implemented in MANETs to facilitate defense against attacks or implement cooperation, decreasing self-centered node behavior. Anomaly detection statistically defines anticipated behavior; it gathers data from genuine user behavior in a defined period, with statistical tests applied to regulate anomalous behavior with a high level of assurance. In real implementation, both approaches—preventive and reactive—are found to be more effective against attacks when combined [11]. The conventional MANET routing protocols assume that all contributors are honest; this directly permits malicious nodes to activate and attempt to paralyze the entire network, simply by providing erroneous information.

Some attacks—such as impersonated nodes, blackhole, and wormhole—are common to all routing protocols, whereas other types are specific to a particular routing algorithm. For instance, in AODV, a malicious node may reply to an RREQ assuming that it has the most recently updated routes to the destined node; however, it may not have. The AODV protocol was designed assuming that all nodes are trustworthy and lack security considerations; this vulnerability is often exploited by intruders. Security enrichments to the AODV protocol are constantly needed. Many scholars have explored this subject: Jasmine et al. evaluated the performance of the AODV protocol under blackhole attacks and no blackhole attacks by calculating the end-to-end delay of packets and the packet delivery rate [12]; the study's results showed that the packet delivery rate of AODV under attack is more than normal. However, the end-to-end delay reduces abruptly when AODV is under attack. Sharma et al. studied the impact of blackhole attacks on MANET performance, and found that the throughput, packet delivery rate, and end-to-end delay of normal AODV are higher than blackhole Attacks [13]. In DSDV, a malicious node may subjectively tamper with the updated messages to interrupt the routing algorithm. In [14], a secure efficient ad hoc distance vector routing protocol (SEAD) based on the insecure DSDV protocol is presentedOLSR. The optimized link-state routing (OLSR) protocol is a proactive routing protocol [3] that offers promising performance in terms of bandwidth and traffic overhead but does not incorporate any security measures. As a result, OLSR is vulnerable to various kinds of attacks [15], such as flooding attacks, link withholding attacks, replay attacks, denial-of-service (DOS) attacks, and collision.

The classical ZRP routing protocol does not use any security mechanism; however, it is employed in many applications where security is predominantly required. As the ZRP is a hybrid protocol, it has the advantages of both preventive and reactive protocols. Researchers have proposed enhanced versions of the ZRP that incorporate security mechanisms [16–18]. Thus, from the literature insights above, it can be inferred that security enhancement in the routing protocols is essential to protect against hostile attacks.

3. Related Work

In MANETs, the outliers can be introduced from several sources, such as hardware/software [19], environment [20], deviance from consistent system arrangement for security conciliation [21], or uncertainty of data [22,23]. These outliers can arise at any level, such as a node, data, or network level [24]; they may be statistical/knowledge-based outliers [25], Markov-/hidden-Markov-based outliers [26], density-based outliers [27–29], distance-based outliers [30–32], or global/semiglobal/distributed outliers [33].

In statistical/knowledge-based outliers, the common methodology to solve the outlier detection problem is built on the construction of probabilistic data models utilizing mathematical methods of applied statistics and probability theory. The outlier detection system, based on a statistical approach, studies the behavior of users through measuring techniques. The system in its running state detects outliers constantly through methods based on regression analysis [25]. A Markov chain is a random process of discrete state space and is described as "the next state is dependent only on the current state and does not depend on how the system has been reached in the current state". Generally, a normal profile using the Markov chain is constructed that captures the temporal dependency among the network activities [26]. The density-based approach was first proposed by Breunig et al. [27]. Such methods evaluate the various density-based distributions of the input keys, and find different outliers as the ones that exist in low-density regions [28]. Such outlier detection methods also evaluate different instances of data at various specified zones; these instances can be determined for distance-based methods of an outlier at a dense zone [29]. Such distance-based detections are calculated for distances for object data with geometric interpretations. For each outlier factor, a function F is specified as F: x → R, where an outlier can be given as object x from different objects R. Various common definitions associated with distance-based outlier detection are provided in [30–32].

As stated, the outliers are introduced in MANETs through various sources and at different levels. Various researchers in the field have faced the challenge of outlier detection: Imani et al. [34] combined misuse detection and anomaly detection to exploit the advantages of both techniques; They used the dynamic programming approach of the hidden Markov model (HMM) to share information history and scheduling in order to save on costs related to security requirements. The simulation results present the efficiency of the proposed scheme. Rammohan [35] proposed a C4.5 clustering-based anomaly detection method; the outcomes show that the proposed method efficiently detects anomalies where the false alarm ratio (FAR) is low, making sure that the detected anomalies are real attacks. Khan et al. [36] proposed a mathematical-model-based adaptive trust threshold (ATT) strategy for isolating misbehaving nodes in MANETs; The findings show that the ATT is robust in comparison with an existing approach in terms of convergence to the same trust threshold value computed at all neighbor nodes for malicious nodes, and is also energy efficient. Lakshmi et al. [37] proposed a method to improve security by an anomaly-based intrusion detection process, and used a zone-based, ad hoc, on-demand distance vector routing protocol to find the shortest path; this method comprises feature selection for anomalous IDs, and identifies new attacks by using decision rules from the database. Qasim et al. [38] used reactive protocols for routing traffic in MANETs, and analyzed anomalous activities to detect outliers that were then matched with ground data; the findings in their study show that a rapid rise in traffic pointed to an anomaly; this is useful for resource and path allocation, as well as fault avoidance. Gomathy et al. [39] proposed a heterogeneous, cluster-based secure routing scheme that offers trust-based secure networks for attack detection—such as wormholes and blackholes instigated by the existence of malicious nodesin MANETs. The simulation outcomes show that the proposed model works effectively for spotting malicious nodes efficiently. The efficiency of the proposed approach is 96% for malicious node detection; it is also 10% more efficient in terms of energy consumption. Narayanan et al. [40] state that clustering is a key routing technique used to reduce energy consumption and, in their work, they propose and evaluate energy-efficient cluster head selection for fault-tolerant routing to reduce single-link failure in MANETs; the simulation results show that the proposed model could implement improved fault tolerance and extend the lifetime of the network.

Venkana et al. [41] propose an algorithm called trust-and-energy-based ad hoc on-demand distance vector; this isolates malicious nodes by dynamic calculation of the trust and energy values of the nodes in the topology, and enhances the routing performance of the AODV algorithm—specifically, the packet delivery ratio and average end-to-end latency. Shan et al. [42] detected selfish nodes through their proposed approach, and quantitatively examined the influences of node selfishness triggered by energy depletion in MANETs in terms of packet loss rate, round-trip delay, and throughput. Gopal Krishnan et al. [43] developed a high-power-saving management system for MANETs via the use of means clustering; they achieved reduced power and energy loss compared to other methods, such as transmission and direct communication protocols; the experimental results suggest that the proposed scheme is suitable to decrease energy dissipation in comparison to other protocols, such as transmission and direct communication protocols. Abdulmunem et al. [44] discussed resource constraints in MANETs, and presented limited energy and system lifetime as challenges faced by MANETs; they give an account of protocols such as the highest degree clustering algorithm (HDCA) and lowest identifier clustering algorithm (LIDCA) under three headings of throughput, network lifetime, and packet delivery ratio; their proposed novel clustering algorithm's simulation results show that it outperforms HDCA and LIDCA in terms of network lifetime and offers effective energy distribution. Arivarasan et al. [45] proposed a form of red deer algorithm (RDA)-based energy-efficient QoS routing for MANETs called RDA-EQRP. RDA finds the shortest path from a source to a destination while preserving energy, in addition to supporting reliability, bandwidth, static resource capacity, quality, and delay; simulation results show that the proposed RDA-EQRP consumes less energy in MANET routing.

4. Proposed Scheme

To isolate or detect outliers in MANETs, the cluster zones are observed. Here, ”Re” is the region chosen for observation during the period from the initial time (Ti) to the termination time (Tt) in one span. Moreover, *TW* = (*Ti*, *Tt*) is the chosen window. $\boldsymbol{T_W^{i-day}} \in \{(\boldsymbol{T_i^1}, \boldsymbol{T_t^1}), (\boldsymbol{T_i^2}, \boldsymbol{T_t^2}), (\boldsymbol{T_i^3}, \boldsymbol{T_t^3}), \ldots, (\boldsymbol{T_i^n}, \boldsymbol{T_t^n})\}$ are the total window sets chosen to observe on the nth day. In the same way, $\boldsymbol{T_W^{x-month}}$ and $\boldsymbol{T_W^{y-year}}$ are the chosen observed windows during the xth month and yth year, respectively. In the proposed model, unsafe outlier levels escalate with an increase in time and performance. The outliers' steps followed are:

1. *Calculate the probability of finding a node in a region "Re"*
   The probability of node ”N$_\mathrm{m}$” existing in a regular region ”Re” for the period of $\boldsymbol{T_{Frame}} \in \left\{\boldsymbol{T_W^{n-day}}, \boldsymbol{T_W^{x-month}}, \boldsymbol{T_W^{y-year}}\right\}$ in the static slot of $\boldsymbol{T_W}$ per $\boldsymbol{T_{Frame}}$ is computed as:
$$\boldsymbol{P_S^{AVG}} = (\mathbf{1}/(\boldsymbol{T_{Frame}} - \mathbf{1}) \sum_{v=1, v=w}^{W} \boldsymbol{P_s}(\boldsymbol{N_m}, \boldsymbol{Re},\ \boldsymbol{T_W^v}) \tag{1}$$
2. *Calculate the probability of finding a node in an expected "Re"*
   The expected presence with timestamp $\boldsymbol{T_S}$ is computed as:
$$\boldsymbol{P_S^{AVG}} = (\frac{\mathbf{1}}{\boldsymbol{T_{Frame}} - \mathbf{1}})(\sum_{v=1, v=w}^{W} (\boldsymbol{N_m}_{\boldsymbol{Active_1}}^{((x_1^i,\, y_1^i) \ldots ((x_1^n,\, y_1^n))} || \boldsymbol{N_m}_{\boldsymbol{Passive_1}}^{((x_1^i,\, y_1^i) \ldots ((x_1^n,\, y_1^n))}) \cdot p_{x_1x_2} p_{x_2x_3} \cdots p_{x_{n-1}x_n}, \text{ Re, } (\boldsymbol{T_{W \ldots\ldots\ldots}^{T_S}} \boldsymbol{T_W^{T_S}})_v \Big) \tag{2}$$
   under the Markov chain, in which each subsequent sequence is dependent on preceding states.
3. *Identify outlier using anomaly score*
   A node is in either an active (source, destination, intermediary, or switching on)—represented as $(\boldsymbol{N_m}_{\boldsymbol{Active'}})$—or passive (sleep, switching-off node) $(\boldsymbol{N_m}_{\boldsymbol{Passive}})$ state. An idle node is not considered to be either an active or passive node. The active or passive states' anomaly scores are computed as:
$$\text{Anomaly Score} = \Big(\boldsymbol{N_m}_{\boldsymbol{Active}}^{\boldsymbol{Attendee}} - \ (\boldsymbol{AVG}_{(\boldsymbol{N_m}_{\boldsymbol{ACTIVE}} + \boldsymbol{N}_{m\boldsymbol{SLEEP}})}^{\boldsymbol{Attendee}}))/\text{STDEV} \tag{3}$$
   where standard deviation (STDEV) is calculated as:
$$Avg = \sum_{k=0}^{n} \frac{S.RR_k}{n} \tag{4}$$

$$V = \sum_{k=0}^{n} \frac{(RR_k - Avg)^2}{n} \tag{5}$$

$$STDEV = \sqrt{V} \tag{6}$$

Standard deviation (STDEV) is calculated using Equation (6). For instance, nodes X1, X2, X3, and X4 broadcast 10, 10, 20, and 100 request packets per second, respectively. X4 is a malicious node. The computed average (Avg), Variance (V), and STDEV are 35, 1425, and 38, respectively.

An outlier has an anomaly score lower than a specific threshold. Algorithms 1–3 are used to calculate the threshold value and for the identification of anomalous node behavior, while Algorithm 4 is used for cluster head selection and identifying outliers by using a threshold value.

Algorithm 1 works for the IDLE link and describes the variation in the threshold for a local event. The anomaly score ($\boldsymbol{Current_{Anomaly}} - \boldsymbol{Last_{Anomaly}}$) is matched with the STDDEV anomaly score value of nodes in the network.

Algorithm 1: Threshold limit for a local event if a link is IDLE

```
if (($Current_{Anomaly} - Last_{Anomaly}$) < $STDEV_{Network}$)
$Current_{Threshold}$ = $STDEV_{UPTO\_CURRENT\_ANOMALY}$
$Last_{Anomaly}$ = $Current_{Anomaly}$;
```

Algorithm 2 considers the QoS parameters (such as link capacity, bandwidth, throughput, packet delivery, end-to-end delay, and energy consumption) in threshold limit calculation. High throughput, link capacity, and bandwidth, as well as lower end-to-end delay and energy consumption, are adequate for a robust network.

Algorithm 2: Threshold limit for a local event if a link is BUSY

```
If ((throughput, link capacity, bandwidth, packet delivery) > QoS_positive_threshold) AND
((end-to-end delay, energy consumption) < QoS_negative_threshold)
if (($Current_{Anomaly} - Last_{Anomaly}$) $\geq$ $STDEV_{Network}$)
$Current_{Threshold}$ = $STDEV_{UPTO\_CURRENT\_ANOMALY}$
$Last_{Anomaly}$ = $Current_{Anomaly}$;
Else
No change in $Last_{Anomaly}$
```

Algorithm 3 explains the scenario where the anomaly score's threshold limit is calculated when packet loss or drop is high. In a high-packet-loss or -drop scenario, the value of the anomaly's score varies exponentially until the packet loss or drop is beyond a threshold. The threshold value of packet loss or drop is the average value of the network's packet loss or drop.

Algorithm 3: Threshold limit for a local event if packet loss is high

```
If ((packet loss or drop) > QoS_negative_threshold)
While((packet loss ) < QoS_negative_threshold)
Set t=0
If (t==0)
$Last_{Anomaly}$ = $Current_{Anomaly}$
Else
$Last_{Anomaly}$ = 2*$Last_{Anomaly}$
Else
No change in $Last_{Anomaly}$
```

Algorithm 4 explains the scenario of identifying the outliers and the selection of cluster heads. The node with the highest energy is selected as a cluster head, and a threshold value is used to identify outliers. This information about the outlier and a node is communicated to the cluster head, as well as to neighbor nodes, in order to avoid communication through the victim node. By doing so, this energy is preserved for nodes at different levels, ensuring the optimization of resources.

The objective of Algorithms 1–3: For outlier detection, the anomaly score threshold limit is calculated.

Algorithm 4: Energy calculation and identification of outliers

```
1.  Set cluster_head = node with the highest energy
2.  Set threshold (value)
3.  If route reply of node (i) > threshold (value)
4.  Send alert to cluster head and neighboring nodes that the node is an outlier
5.  If the node is an outlier, then avoid routing through it
6.  Calculate energy discharge
```

Like outlier detection at the local level, outliers are also identified at the global or network levels, as shown in Figure 2.

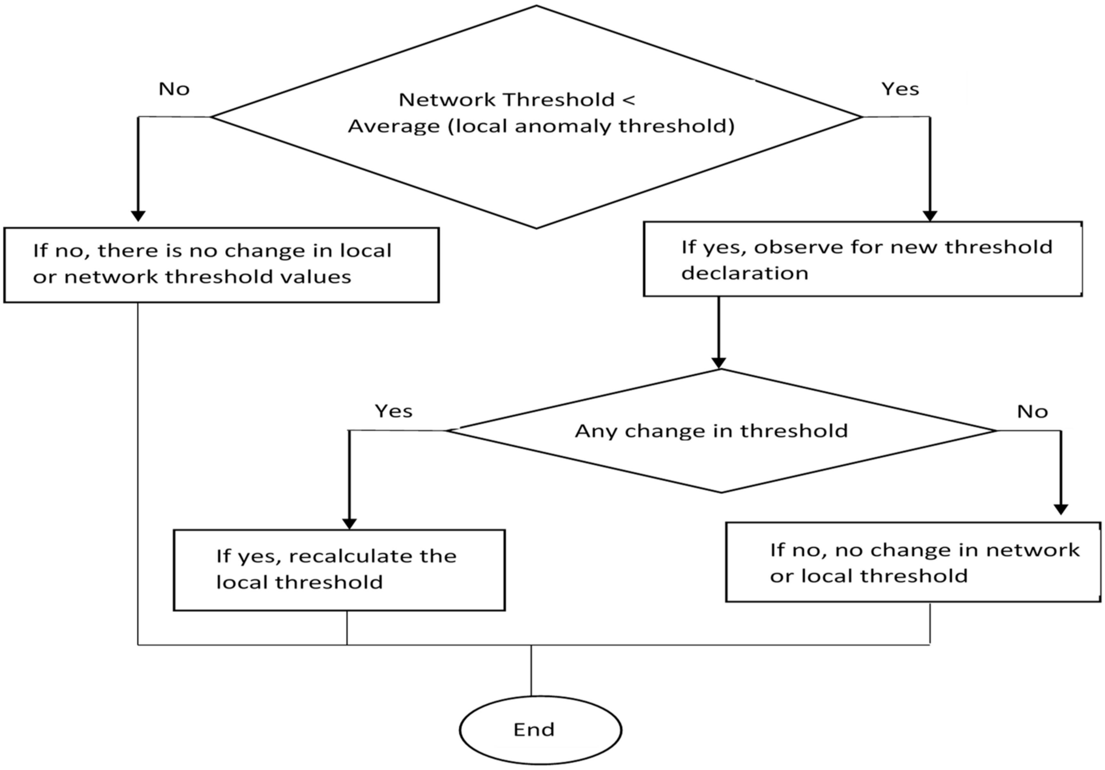
No
Network Threshold <
Average (local anomaly threshold)
Yes
If no, there is no change in local or network threshold values
If yes, observe for new threshold declaration
Yes
Any change in threshold
No
If yes, recalculate the local threshold
If no, no change in network or local threshold
End

Figure 2. The proposed approach for outlier detection.

5. Simulation Results

In this section, the results and analysis (for the detection ratios and QoS parameters) of the study are presented.

In the real-world environment, protocol testing involves huge costs, and is very time-consuming. Simulation tools are a good choice to create a scenario for the performance evaluation of a network, because of the dynamic nature of MANETs. In this article, we use the network simulation tool ns-3; ns-3 is a free, open-source discrete-event network simulator; ns-3 is widely used, as it is open source, operates in a high degree of complex network environment, and offers high reliability; its simulation results can be easily reproduced and analyzed; it is also cost-effective for constructing an application.

In the ns-3 simulator, the AODV, DSDV, DSR, OLSR, and ZRP routing protocols were implemented and the performance matrix was calculated. The analysis was carried out in terms of the impact on MANET performance and anomaly detection, in order to enhance security when the density of the network is increased.

To perform analysis of the AODV, DSDV, DSR, OLSR, and ZRP routing protocols using the ns-3 network simulation tool, several parameters were applied; these parameters were used to calculate and analyze the performance of the network (Table 1). ns-3 provides different frameworks and built-in libraries; these libraries can be linked to the (C++/Python) simulator program, either statically or dynamically. In this work, the ns-3 simulator Python language is used in conjunction with LINUX OS.

Table 1. Simulation parameters.

Parameters	Value
Numbers of nodes	200–1000
Channel type	Wireless channel
Radio propagation model	Ray tracing
Network interface	Wireless PHY
MAC type	802.11
Interface queue	Priority queue
Antenna	Omni antenna
Max packet in queue	50
Dimension	1000 m × 1000 m
Mobility model	Random waypoint mobility
Data rates	5 packets/second
Packet size	512 bits
Simulator	ns-3
Simulation time	5000 s
Number of slots assigned to the reader at stretch( )	1
Time of each slot	10 ms
Velocity(minimum to maximum)	0.3–5 m/s

The various notations used in the proposed methodology are described in Table 2. The simulation results of each routing protocol in the ns-3 environment have been fetched and presented in graphs (Figures 3–7) and data tables (Tables 3 and 4). According to the simulation results, there is a clear indication that when the network density increases, the routing protocols under study are affected in terms of QoS. The comparative analysis of the routing protocols shows that the performance of the ZRP is enhanced concerning jitter value, end-to-end delay, throughput, and average energy consumption.

Table 2. Summary of notations.

Notations	Meaning
Re	Region
Ti	Initial time
Tt	Termination time
TW	Window selected in one stretch
$\mathbf{N_m}$	Mobile node
T_S	Timestamp
T_{Frame}	Timeframe
P_S^{AVG}	Probability of finding a node in a region
$N_{m_{Active'}}$	Active node
$N_{m_{Passive}}$	Passive node
$STDEV$	Standard deviation

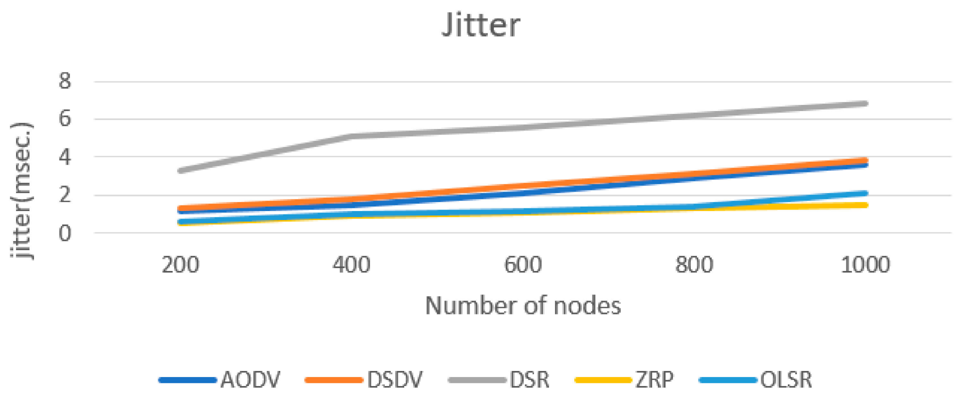

Figure 3. Comparative analysis of jitter in 200–1000-node networks using the proposed scheme over five MANET routing protocols.

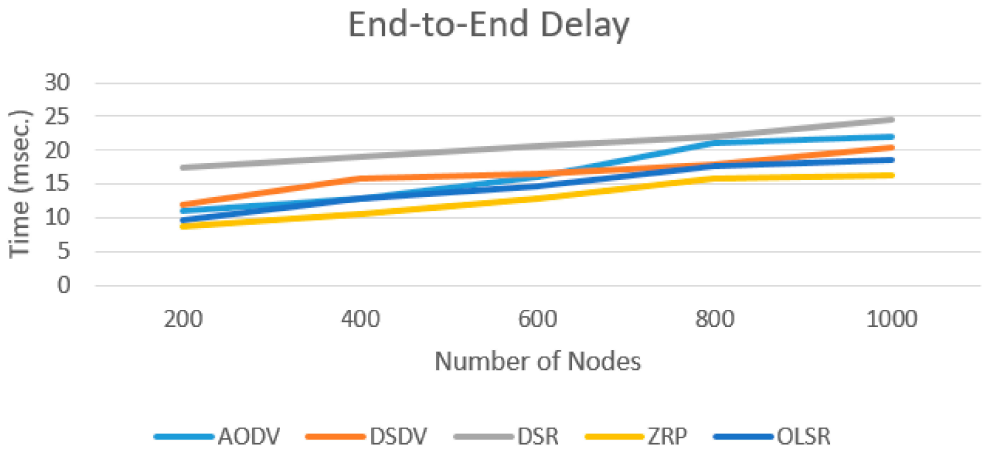

Figure 4. Comparative analysis of end-to-end delay in 200–1000-node networks using the proposed scheme over five MANET routing protocols.

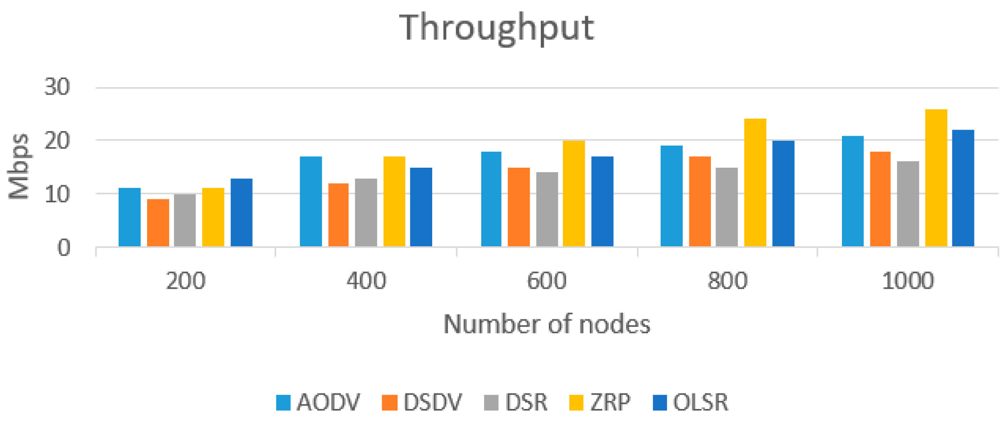

Figure 5. Comparative analysis of throughput in 200–1000-node networks using the proposed scheme over five MANET routing protocols.

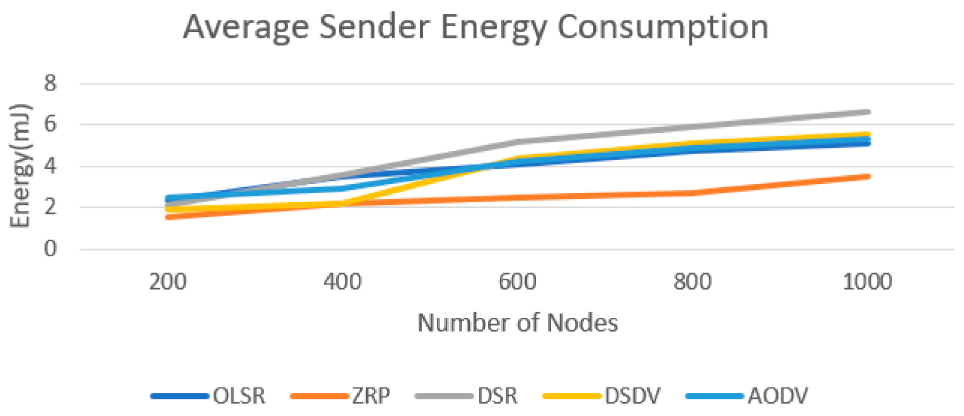

Figure 6. Comparative analysis of average sender energy consumption in 200–1000-node networks using the proposed scheme over five MANET routing protocols.

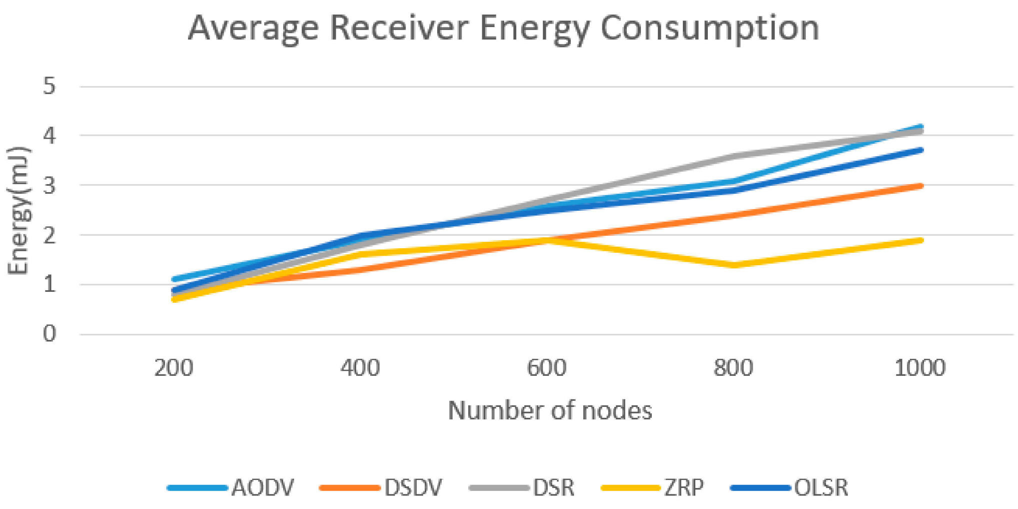

Figure 7. Comparative analysis of average receiver energy consumption in 200–1000-node networks using the proposed scheme over five MANET routing protocols.

Table 3. Comparative analysis of detection ratios with variations in the number of nodes.

	N = 200	N = 400	N = 600	N = 800	N = 1000
ADR	0.741	0.715	0.711	0.693	0.665
WCAR	0.080	0.11	0.12	0.14	0.16
ALADR	0.730	0.700	0.683	0.672	0.651
ALWCAR	0.055	0.07	0.08	0.09	0.10
ALWCAR–WCAR	0.025	0.04	0.04	0.05	0.06
ALADR-ADR	0.011	0.015	0.028	0.021	0.014

Table 4. Comparative detection ratio analysis at network level.

		N = 1000	
Parameter	**Yang et al. [26]**	**Branch et al. [33]**	**Proposed Approach**
Minimum ADR	48.8%	57.8%	66.5%
Minimum WCAR	9%	10%	8%
Minimum ALADR	0.1%	0.2%	0.6%
Minimum ALWCAR	≤0.1%	≤0.2%	≤0.6%

A. *Comparative Analysis of Detection Ratios*

To analyze the performance, the ns-3 simulator was used. In addition to the ns-3 simulator, Python language was used on LINUX OS.

The variation in the number of nodes on ns-3 was 200–1000 for the zone routing protocol (ZRP) for 5000 s. The comparison of detection ratios with node variation is presented in Table 3.

(i) Anomaly detection ratio (ADR)

$$ADR = \frac{anomalies\ detected\ by\ proposed\ system}{number\ of\ anomalies\ in\ trace\ file}$$

As the number of nodes increases, the value of ADR decreases; its minimum value is 66.5% in a 1000-node network. The reason for the decrease in ADR value is that, after transmitting control packets, many nodes become silent.

(ii) Wrongly calculated anomaly ratio (WCAR)

$$WCAR = number\ of\ inliers\ detected\ as\ outliners$$

As the number of nodes increases, the value of WCAR also increases, ranging from 8% for 200 nodes to 16% for 1000 nodes.

(iii) Average local anomaly detection ratio (ALADR)

$$ALADR = \frac{value\ of\ ADR\ collected\ from\ each\ local\ subgroup}{number\ of\ local\ subgroup}$$

The value of ALADR < ADR, and further declines with an increasing number of nodes. The different values of ALADR and ADR indicate the presence of outliers in the network that are not constituents of any local subgroup. The minimum and maximum values are 1.1% and 1.4% for 200 and 1000 nodes, respectively.

(iv) Average local wrongly calculated anomaly ratio (ALWCAR)

$$ALWCAR = \frac{acum\ of\ WCAR\ values\ from\ each\ local\ subgroup}{number\ of\ local\ subgroups}$$

Here, ALWCAR < WCAR, and ALWCAR increases with an increase in the number of nodes.

To appraise ADR, WCAR, ALADR, and ALWCAR in real implementation:

ADR is one of the important factors to influence the performance of the network by detecting anomalies on time; WCAR should be minimal, as it constitutes the incorrect identification of inliers as outliers, which may significantly affect the performance in terms of energy consumption and security; ALADR is the parameter that helps to identify the outlier at the local subgroup level and network levels.

B. *Comparative Analysis of QoS Parameters*

Figures 3–7 show the performance analysis of the proposed outlier detection mechanism over five MANET routing protocols using various QoS parameters in a network of 200–1000 nodes. The QoS parameters taken for performance analysis were jitter, end-to-end delay, throughput, and sender and receiver energy consumption. The five MANET routing protocols selected for analysis were destination-sequenced distance vector (DSDV) routing, ad hoc on-demand distance vector (AODV), dynamic source routing (DSR), optimized link-state routing (OLSR), and the zone-based routing protocol (ZRP). The observations of QoS parameters were as follows:

Figure 3 shows the comparative analysis of jitter in 200–1000-node networks using the proposed outlier detection mechanism over five MANET routing protocols. The findings reveal the lowest jitter value for the ZRP—a hybrid protocol that acclimatizes to dynamic settings of the network. As the number of nodes rises, the jitter value also increases. The reason for the increase in jitter value is the rise in traffic, which results in increased overhead in the network.

Figure 4 shows the comparative analysis of end-to-end delay in 200–1000-node networks using the proposed outlier detection mechanism over five MANET routing protocols. For end-to-end delay, the ZRP has the lowest value, while DSR has the highest value; with the rise in node numbers, the value of end-to-end delay rises; this is because of processing and propagation delays due to an increase in traffic that necessitates more processing time for the large number of requests received.

Figure 5 shows the comparative analysis of throughput in 200–1000-node network using the proposed outlier detection mechanism over five MANET routing protocols. With the rising number of nodes, throughput also increases; this is because there are several paths available to connect to the destination, and this, in turn, increases the probability of successful transmission. Among the five studied protocols, the ZRP breaks unidentified communication by creating different zones that become accustomed to dynamic settings in the network. Hence, the ZRP performs better in comparison to AODV, DSDV, DSR, and OLSR.

Figure 6 shows that average sender energy consumption is lowest for the ZRP and highest for the DSR protocol. This is because the ZRP makes a structured, connected, semi-hierarchical network that facilitates well-timed message delivery. In other protocols, the senders involved packet retransmission due to packet loss or discard in the unstructured network.

Figure 7 shows the comparative analysis of receiver energy consumption in 200–1000-node networks using the proposed outlier detection mechanism over five MANET routing protocols. The ZRP has the lowest value for average receiver consumption, as the network is structured—unlike other protocols, where it is unstructured. Unstructured networks have a higher probability of retransmission or loss of packet acknowledgment.

C. *Comparative Analysis of the Proposed Approach with Existing Mechanisms*

Table 3 presents the comparative account of detection ratios when the number of nodes is varied. The ADR value decreases in the 1000-node network, reaching a minimum value of 66.5% due to nodes being silent after control packet transmission. The value of WCAR for the 1000-node network is maximal—i.e., 16%; hence, the rise is observed when the number of nodes varies from 200 to 1000. In addition, the ADR value is greater than

ALADR when the number of nodes increases, because outliers are detected that do not belong to a local subgroup.

The proposed scheme performs better than the other schemes [26,33] described in the literature, considering the comparison parameters of ALWCAR, ADR, ALDR, and WCAR. DD-ZRP performs better at the local subgroup level and network level, as shown in Tables 4 and 5, respectively.

Table 5. Comparative detection ratio analysis at subgroup level.

	N = 1000		
Parameter	**Yang et al. [26]**	**Branch et al. [33]**	**Proposed Approach**
Minimum ADR	42.5%	51.7%	59.6%
Minimum WCAR	10%	9%	7%
Minimum ALADR	0.3%	0.5%	0.7%
Minimum ALWCAR	≤0.2%	≤0.3%	≤0.6%

To summarize, in this work outliers are detected in resource-constrained key management networks, and a lightweight key management network is constructed to ensure confidentiality, authentication, and integrity in outlier detection. The work is an extension of Teo and Tan's model, in which outlier detection is incorporated to construct a secure network. The hybrid approach of DD-ZRP was designed by integrating three well-accepted protocols proposed by Teo and Tan [1], Traag et al. [2], and Cerpa et al. [3]. The simulation was performed using NS-3, and the proposed algorithms take link state and QoS parameters such as packet drop and energy consumption in the network into consideration in order to detect outliers. To identify outliers in a network, cluster zones in the network were put under observation.

Algorithm 1 explains the variation in threshold limit for the local event if the link is IDLE; in this algorithm, the anomaly score is compared with the threshold value to identify outliers. Algorithm 2 observes the QoS parameters in threshold limit calculation. QoS parameters such as throughput, link capacity, bandwidth, and packet delivery are considered for positive results, while end-to-end delay and energy consumption are considered for negative results. Higher positive results or lower negative results are acceptable for high-performing networks. Algorithm 3 explains the scenario where the anomaly score's threshold limit is calculated when packet loss or drop is high. In a high-packet-loss or -drop scenario, the value of the anomaly's score varies exponentially until the packet loss or drop is beyond a certain threshold. In this work, along with outlier detection at the local level, outliers are also identified at the network level.

On comparing the network outlier detection threshold with the average value of the local threshold, if the network threshold value is lower than it is recomputed after days and weeks to record observations. This process keeps going on until the network threshold value is higher than the average value of local subgroups, as a network must have an equal or higher number of nodes compared to the total number in all subgroups. Algorithm 4 selects the node with the highest energy as the cluster head, and by comparing the route reply of a node with the threshold, an outlier is detected and an alert to the cluster head and the neighboring node is set. The results are compared with the studies of Yang et al. [26] and Branch et al. [33], using the ADR, WCAR, ALADR, and ALWCAR parameters at the subgroup and network levels.

6. Conclusions

MANETs are a challenging research field because of their characteristics, such as dynamic topology, flexibility, open medium, and constrained capability. This makes MANETs pertinent to various applications. However, these features are a threat to the security of the system. Specifically, it is routing that is significant in the security of the entire network; this appears to be a non-trivial problem that cannot be solved effortlessly, i.e., MANETs are much more vulnerable to security attacks. In this paper, we have reviewed the state-of-the-art security protocols in MANETs. Although various researchers have proposed solutions to address the security and performance issues in MANETs, these proposed solutions are not comprehensive for effective and efficient performance and routing security; there are limitations on all solutions.

In this research, we have compared all of the protocols in the ns-3 simulation environment using jitter, throughput, average end-to-end delay, and anomaly detection. For the proposed DD-ZRP approach, a minimum 66.5% anomaly detection ratio is observed in a network of 1000 nodes. A minimum WCAR of 8% for 200 nodes and a maximum WCAR of 16% for 1000 nodes are observed. For ALADR, a minimum of 1.1% outlier for 200 nodes, and a maximum of 1.4% outlier for 1000 nodes, are present in a network that is not part of any subgroup. The ratios shown have significant improvement compared to the prevailing mechanisms. The ZRP protocol—being a hybrid protocol—exploits the advantages of both proactive and reactive approaches, and thus performs better for QoS and outlier detection mechanisms when compared to the other protocols considered in the study. The proposed ZRP-based approach is better for outlier detection with respect to end-to-end delay, jitter, sender/receiver energy consumption, and throughput for 200–1000-node networks. The findings reveal that QoS parameters rise with an increase in the number of nodes in the network. In effect, DSR outperforms at a lower level; however, the pre-eminent routing protocol is the ZRP.

Future studies could consider facilitating a protection mechanism to learn from experience and use the knowledge gained to detect novel intrusive activities. The development and deployment of network security policies is vital in MANETs; this is a further potential area of research. In addition, it would be interesting to investigate this method for other relevant types of applications and evaluate it in a realistic scenario, as this work has only included simulation results. As a final point, the attacks on existing protection schemes make it necessary to enhance existing solutions and make them more robust in order to combat new vulnerabilities introduced into the system.

Author Contributions: Conceptualization, N.C.; methodology, N.C. and G.S.T.; validation, N.C., R.S.B.; formal analysis, N.C.; investigation, N.C. and G.S.T.; data curation, N.C.; writing—original draft preparation, N.C.; writing—review and editing, all; supervision, G.S.T., N.S.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Teo, J.C.M.; Tan, C.H. Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks. In Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks—PE-WASUN '05, Montreal, QC, Canada, 10–13 October 2005; ACM Press: Montreal, QC, Canada, 2005; p. 114.
2. Traag, V.A.; Browet, A.; Calabrese, F.; Morlot, F. Social Event Detection in Massive Mobile Phone Data Using Probabilistic Location Inference. In Proceedings of the 2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing, Boston, MA, USA, 9–11 October 2011; pp. 625–628.
3. Habitat Monitoring: Application Driver for Wireless Communications Technology. *Proceedings of the Workshop on Data communication in Latin America and the Caribbean—SIGCOMM LA '01* **2001**, 20–41.
4. Kiess, W.; Mauve, M. A Survey on Real-World Implementations of Mobile Ad-Hoc Networks. *Ad Hoc Netw.* **2007**, *5*, 324–339. [CrossRef]
5. Hogie, L.; Bouvry, P.; Guinand, F. An Overview of MANETs Simulation. *Electron. Notes Theor. Comput. Sci.* **2006**, *150*, 81–101. [CrossRef]
6. Perkins, C.; Belding-Royer, E.; Das, S. *Ad Hoc On-Demand Distance Vector (AODV) Routing*; RFC Editor 2003; The Internet Society: Reston, VA, USA, 2003; p. RFC3561.
7. AL-Dhief, F.T.; Sabri, N.; Salim, M.S.; Fouad, S.; Aljunid, S.A. MANET Routing Protocols Evaluation: AODV, DSR and DSDV Perspective. In Proceedings of the MATEC Web of Conferences, Penang, Malaysia, 23 February 2018; Volume 150, p. 06024.

8. He, G. *Destination-Sequenced Distance Vector (DSDV) Protocol*; Networking Laboratory, Helsinki University of Technology: Helsinki, Finland, 2002; p. 135.
9. Beijar, N. *Zone Routing Protocol (ZRP)*; Networking Laboratory, Helsinki University of Technology: Helsinki, Finland, 2002; pp. 1–12.
10. Sinha, P.; Krishnamurthy, S.V.; Dao, S. Scalable Unidirectional Routing with Zone Routing Protocol (ZRP) Extensions for Mobile Ad-Hoc Networks. In Proceedings of the 2000 IEEE Wireless Communications and Networking Conference. Conference Record (Cat. No. 00TH8540), Chicago, IL, USA, 23–28 September 2000; IEEE: Chicago, IL, USA; pp. 1329–1339.
11. Joshi, P. Security Issues in Routing Protocols in MANETs at Network Layer. *Proc. Comput. Sci.* **2011**, *3*, 954–960. [CrossRef]
12. Jeni, P.R.J.; Vimala Juliet, A.; Parthasarathy, R.; Messiah Bose, A. Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET. In Proceedings of the International Conference on Smart Structures and Systems—ICSSS'13, Chennai, India, 28–29 March 2013; pp. 178–182.
13. Sharma, S.; Gupta, R. Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks. *J. Eng. Sci. Technol.* **2009**, *4*, 8.
14. Hu, Y.-C.; Johnson, D.B.; Perrig, A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. *Ad Hoc Netw.* **2003**, *1*, 175–192. [CrossRef]
15. Marimuthu, M.; Krishnamurthi, I. Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks. *J. Commun. Netw.* **2013**, *15*, 31–37. [CrossRef]
16. Rajput, S.S.; Trivedi, M.C. Securing Zone Routing Protocol in MANET Using Authentication Technique. In Proceedings of the 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, India, 14–16 November 2014; pp. 872–877.
17. Selvi, S.A.; Vijayaraj, A. Increasing Quality of Service in Video Traffic Using Zone Routing Protocol in Wireless Networks. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–5.
18. Samar, P.; Pearlman, M.R.; Haas, Z.J. Independent Zone Routing: An Adaptive Hybrid Routing Framework for Ad Hoc Wireless Networks. *IEEE ACM Trans. Netw.* **2004**, *12*, 595–608. [CrossRef]
19. Chen, J.; Kher, S.; Somani, A. Distributed Fault Detection of Wireless Sensor Networks. In *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks—DIWANS '06*; Los Angeles, CA, USA, 26 September 2006, ACM Press: New York, NY, USA, 2006; pp. 65–72.
20. Luo, X.; Dong, M.; Huang, Y. On Distributed Fault-Tolerant Detection in Wireless Sensor Networks. *IEEE Trans. Comput.* **2006**, *55*, 58–70. [CrossRef]
21. Ding, M.; Chen, D.; Xing, K.; Cheng, X. Localized Fault-Tolerant Event Boundary Detection in Sensor Networks. In Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005; Voume 2, pp. 902–913.
22. Krishnamachari, B.; Iyengar, S. Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection in Wireless Sensor Networks. *IEEE Trans. Comput.* **2004**, *53*, 241–250. [CrossRef]
23. Martincic, F.; Schwiebert, L. Distributed Event Detection in Sensor Networks. In Proceedings of the 2006 International Conference on Systems and Networks Communications (ICSNC'06), Tahiti, French Polynesia, 29 October–3 November 2006; p. 43.
24. Jurdak, R.; Wang, X.R.; Obst, O.; Valencia, P. Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies. In *Intelligence-Based Systems Engineering*; Tolk, A., Jain, L.C., Eds.; Intelligent Systems Reference Library; Springer: Berlin/Heidelberg, Germany, 2011; Volume 10, pp. 309–325. ISBN 978-3-642-17930-3.
25. Zhang, Y.; Meratnia, N.; Havinga, P. Outlier Detection Techniques for Wireless Sensor Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2010**, *12*, 159–170. [CrossRef]
26. Yang, J.; Wang, Y.L. A New Outlier Detection Algorithms Based on Markov Chain. *Adv. Mater. Res.* **2011**, *366*, 456–459. [CrossRef]
27. Breunig, M.M.; Kriegel, H.-P.; Ng, R.T.; Sander, J. LOF: Identifying Density-Based Local Outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 15–18 May 2000; p. 12.
28. Koufakou, A.; Georgiopoulos, M. A Fast Outlier Detection Strategy for Distributed High-Dimensional Data Sets with Mixed Attributes. *Data Min. Knowl. Disc.* **2010**, *20*, 259–289. [CrossRef]
29. Jain, A.K.; Murty, M.N.; Flynn, P.J. Data Clustering: A Review. *ACM Comput. Surv.* **1999**, *31*, 264–323. [CrossRef]
30. Hawkins, D.M. *Identification of Outliers*; Chapman and Hall: London, UK, 1980; Volume 11.
31. Knorr, E.M.; Ng, R.T. *Algorithms for Mining Distance-Based Outliers in Large Datasets*; University of British Columbia: Vancouver, BC, Canada, 1998; Volume 98, pp. 392–403.
32. Ramaswamy, S.; Rastogi, R.; Shim, K. Efficient Algorithms for Mining Outliers from Large Data Sets. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 15–18 May 2000; pp. 427–438.
33. Branch, J.W.; Giannella, C.; Szymanski, B.; Wolff, R.; Kargupta, H. In-Network Outlier Detection in Wireless Sensor Networks. *Knowl. Inf. Syst.* **2013**, *34*, 23–54. [CrossRef]
34. Imani, M. A Novel Approach to Combine Misuse Detection and Anomaly Detection Using POMDP in Mobile Ad-Hoc Networks. *Int. J. Inf. Electron. Eng.* **2015**, *5*. [CrossRef]
35. Rammohan, S.R. Anomaly Detection in Mobile Ad Hoc Networks(MANET) Using C4.5 Clustering Algorithm. *Int. J. Inf. Technol. Manag. Inf. Syst.* **2015**, 1–10.

36. Khan, M.S.; Midi, D.; Khan, M.I.; Javaid, N.; Bertino, E. Isolating Misbehaving Nodes in MANETs with an Adaptive Trust Threshold Strategy. *Mobile Netw. Appl.* **2017**, *22*, 493–509. [CrossRef]
37. Prasanna Lakshmi, G.S.; Patil, S.B.; Patil, P. Anomaly Detection in MANET Using Zone Based AODV Routing Protocol. In *Advanced Informatics for Computing Research*; Luhach, A.K., Singh, D., Hsiung, P.-A., Hawari, K.B.G., Lingras, P., Singh, P.K., Eds.; Communications in Computer and Information Science; Springer: Singapore, 2019; Volume 956, pp. 454–468. ISBN 9789811331428.
38. Jabbar Qasim, N.; Majeed Mohammed, S.; Sami Sosa, A.; Albarazanchi, I. Reactive Protocols for Unified User Profiling for Anomaly Detection in Mobile Ad Hoc Networks. *Period. Eng. Nat. Sci.* **2019**, *7*, 843. [CrossRef]
39. Gomathy, V.; Padhy, N.; Samanta, D.; Sivaram, M.; Jain, V.; Amiri, I.S. Malicious Node Detection Using Heterogeneous Cluster Based Secure Routing Protocol (HCBS) in Wireless Adhoc Sensor Networks. *J. Ambient Intell. Hum. Comput.* **2020**, *11*, 4995–5001. [CrossRef]
40. Narayanan, A.E.; Devi, R.; Jayakumar, D.A.V. An Energy Efficient Cluster Head Selection For Fault Tolerant Routing in MANET. *Int. J. Eng. Technol.* **2013**, *5*, 9.
41. Venkanna, U.; Agarwal, J.K.; Velusamy, R.L. A Cooperative Routing for MANET Based on Distributed Trust and Energy Management. *Wireless Pers. Commun.* **2015**, *81*, 961–979. [CrossRef]
42. Shan, A.; Fan, X.; Wu, C.; Zhang, X.; Fan, S. Quantitative Study on the Impact of Energy Consumption Based Dynamic Selfishness in MANETs. *Sensors* **2021**, *21*, 716. [CrossRef] [PubMed]
43. Krishnan, C.; Gomathi, S.; Anusha Bamini, A.M. High Energy Efficient Lifetime Management System and Trust Management Framework for Manet Using Self-Configurable Cluster Mechanism. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1229–1241.
44. Al-Najjar, A.A.M.; Chasib, H.S.; AL-Ogaili, I.J.K. Optimizing MANETs Network Lifetime Using a Proactive Clustering Algorithm. *TURCOMAT* **2021**, *12*, 3280–3292. [CrossRef]
45. Arivarasan, S.; Prakash, S.; Surendran, S. An Energy Efficient Qos Routing Protocol Based On Red Deer Algorithm in MANET. *TURCOMAT* **2021**, *12*, 1461–1471. [CrossRef]