A Novel Intrusion Detection Algorithm: An AODV Routing Protocol Case Study

Gurveen Vaseer[1], Garima Ghai[2] and Pushpinder Singh Patheja[3].
Department of Computer Science and Engineering, Oriental University, Indore.[1,2]
Department of Computer Science and Engineering, VIT University, Bhopal.[3]
Email-ID: gurveenv@orientaluniversity.in[1], garimaghai@orientaluniversity.in[2]
and pspatheja@gmail.com[3].

***Abstract*— Mobile ad-hoc network (MANET) is a collection of movable nodes capable of self-routing, constraining energy and decentralized handling of nodes. It faces many challenges due to uncertainty of network topology i.e. security and congestion. In this paper we propose a novel algorithm for intrusion detection against attacks such as probing, Denial-of-service (DoS), vampire and User-To-Root (U2R) in a MANET environment. The attack detection has been carried out using a profile (behavior) analysis and a confusion matrix (True positives, True negatives, False positives, False negatives). The performance of a standard Ad hoc On-Demand Distance Vector (AODV) routing protocol has been reported for all 4 types of attack in a network simulator-2 (ns-2) environment. To the best of authors' knowledge, this is the first paper reporting a novel intrusion detection algorithm using behavior analysis for an AODV protocol in a MANET environment.**

I. Introduction and Contributions

Mobile ad-hoc network (MANET) is the most promising and rapidly growing technology that is primarily based on a self-organized and speedily deployed network [1]. As a result of its features, MANET is more suitable for real world applications in which the network topology changes quickly. Nodes in MANETs join and leave the network dynamically exhibiting their independent and self-deployable behavior. No mounted set of infrastructure and centralized administration is required in this kind of a network. Nodes are interconnected through wireless interfaces. The dynamic nature of such networks makes it extremely vulnerable to varied link attacks. The basic requirements for secured networking are protocols that guarantee confidentiality, handiness, legitimacy and integrity of network [2].

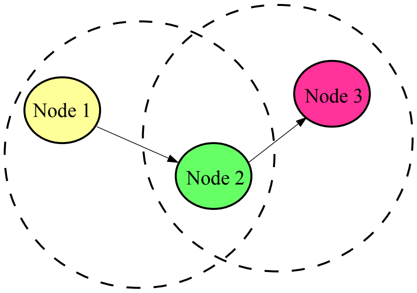


Fig. 1. Representation of a mobile ad hoc network (MANET)

Figure 1 shows the composition of MANET where 3 different, independent nodes communicate with each other in different environments through another independent node. Several existing security solutions for wired networks are ineffective and inefficient for MANET environment because the transmission takes place in an open space making the MANETs more susceptible to security attacks. There are 4 major kinds of security attacks viz. Denial of Service(DoS), probing, vampire and User-to-Root (U2R) [3]. In DoS attack, the system is flooded with unwanted traffic so that legitimate users cannot it hence crashing the server [4]. In probing, a device or an activity can be introduced in the system to gain access of the system hence damaging it. In U2R, the attacker gains local access to the victim machine and tries to gain super user privileges [5]. Vampire attack is a type of DoS attack, but it consumes the node's energy and decreases the network efficiency and reliability. In the presence of a security protocol, effectiveness of various attacks will be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication depends a lot on the collaboration of the concerned mobile nodes [1]. Ad hoc On-demand Distance Vector (AODV) routing protocol is an on-demand protocol i.e. it discovers routes on and as needed basis using route discovery process [6].

The AODV protocol is initiated when a node wants to communicate with other nodes outside its range. In this, first unicast routes are determined to the destination. Then, messages are sent to nodes with the following message types: RREQ (route request), RREP (route reply) and RERR (route error). RREQ is generated when a node needs to find a route to the destination and has the sequence number of the destination. RREP is generated if the destination is reached or a path has been traced by the node. RERR is generated for broken links in the path. Each node maintains a route table that contains information about reaching destination nodes. Destination information is assured by comparing the sequence number of the incoming AODV message with the sequence number for that destination. The process continues till the route is complete and source nodes and destination nodes are well routed.

The *novel contributions* of this paper are as follows:

1) A novel intrusion detection algorithm for a MANET environment is proposed.
2) The algorithm is designed to detect probing, Denial-of-service (DoS), vampire and User-To-Root (U2R) attacks.
3) The proposed algorithm uses profile (behavior) analysis and confusion matrix for detection.
4) The impact of the attacks is studied using AODV protocol.

The remainder of the paper is organized as follows: Section II presents the related research. Section III presents the proposed research and discusses the proposed algorithm. Section IV discusses the output responses of the network under normal (no attack) and abnormal (under attack) conditions. This is followed by conclusions and future research in section V.

II. Related Research

In this section we discuss the existing research in the area of MANET security against probing, vampire, DoS and U2R attacks. Authors in [7] present a real-time intrusion detection system (IDS) using the Multi-agent System (MAS-IDS) to reduce the time of process traffic information network. Furthermore, the analysis of enormous amounts of information in the system within the shortest possible time has been achieved. Swati Paliwal et. al.[8] propose a methodology that supports Genetic formula for detection of inquisitor, Denial of Service(DoS) and Remote to User (R2L) attacks. The planned approach aims at gaining detection of the inquisitor, R2L and DoS attacks with minimum false positive rate. Out of the total intrusions in testing dataset, detection of more than 97% of the intrusions is anticipated by this approach. Distributed intrusion detection architecture proposed by Jaydip Sen [9] supports autonomous and cooperating agents with no centralized analysis parts. The agents collaborate by using a gradable communication of interests and information, and therefore the analysis of intrusion information is formed by the agents at the bottom level of the hierarchy. S. T. Sheu et.al. [10] present a secured routing methodology for police work that prevents network attacks like false reports and Gray-hole attacks in wireless device networks. Authors in [11] discuss the energy efficient protocols that divide the network to efficiently maintain the energy consumption of sensing element nodes. D.R. Raymond et al. [12] discuss the denial-of-sleep attacks at the MAC layer. Authors in [13] propose a methodology that aims to extend the lifetime of power-constrained networks by using less energy to transmit and receive packets. S. S. George et. al. [14] present a routing protocol to bind the harm caused by vampires within the forwarding phase. Table I summarizes the comparison of the proposed research in this paper with existing literature.

III. Proposed Work

The proposed work detects the four types of attacks i.e. probing, DoS, vampire and U2R in MANETs. All the above listed attacks have been detected through specific behavior analysis based methodology. The detection engine creates two tables, one containing the normal profile such as TCP, UDP, AODV related formats and the other is abnormal table containing the behavior of abnormality such as probing, vampire, DoS and U2R. If the abnormality matches with a particular attack, the attacks are classified in that particular class which helps in detection of each attack through this analysis. In our simulation engine, the packet format for TCP, UDP are fixed i.e. in the header part TCP/UDP will be specified. If the header part is missing or does not match with the standard TCP/UDP/AODV formats implies that it is a hampered packet. For simulation purposes, separate environments have been created for the 4 types of attacks. For a multiple attack scenario, we may utilize the unique categorization techniques of each attack for detection [15]. The complete algorithm is discussed in subsection III-A.

A. Proposed Algorithm

In this subsection we describe the proposed detection algorithm which detects all four types of attacks (vampire, probing, DoS, U2R). The algorithm is divided into three sections viz. input, procedure and output shown in algorithm 1.

In the proposed algorithm 1, data is tested using 50 nodes in a range of 800 × 800 m. Here, I is a collection of addresses of intermediate nodes between sender and receiver. It is compared with R (receiver node's address) until there is a match. Once there is a match, rpkt, which is a routing packet, is received by I and forwarded until it reaches the destination node. Because network related communication is possible with both Transport, Communication and Application layers, we have grouped TCP/UDP and AODV. Data is classified as normal and abnormal depending on the packet header that the network generates; those with standard TCP/UDP/AODV headers will be classified as normal and the rest can be presumed as abnormal. Attack detection is done through behavioral analysis; when data is passed through the simulation engine if data == b_h(n) then no traces of abnormal data are found hence no attack has occurred. If data == b_h(ab) then an attack has occurred which can be of four types:

1) If data is being captured then it is a probing attack.
2) If junk messages are getting transmitted and they do not match TCP,UDP standards then attack type is DoS.
3) If there is abnormal energy consumption and the path is disabled, it is vampire attack.
4) If IP is being modified then it is a U2R attack.

Figure 2 shows the flowchart for the proposed algorithm. Once the attacks are detected, we can start counterattack measures. Counter attack measures can be designed by analysis of respective behavior of the 4 attacks. This can be done by abolishing suspicious nodes and hence ensuring secure communication between sender and receiver nodes [15].

Table II shows the behavior table, where S: send, R: Receives, F: Forward, D: Drop, N: Normal, H: High. When there is absence of attacks, all the protocol values (TCP,UDP,AODV) are satisfied hence generate a positive acknowledgement to the receiver and the queue utilization is normal. Whereas in any of the attack scenarios based on behavioral conditions, there is drop in packets, no acknowledgement is sent and queue

TABLE I

COMPARISON WITH RELATED WORKS

Reference	Work done	This work
Yaseen [7]	MAS-IDS to reduce time complexity of network	Detects 4 major attacks
Paliwal [8]	Attack free environment using genetic formula	Attack free environment using behavior analysis
Sen [9]	Distribution intrusion detection architecture minimizes intrusions	Remove intrusions
Sheu [10]	Prevention of grey hole attacks	Detection of 4 attacks
Doshi [13]	Optimization of energy using power constrained networks	Removal of attacks
George [14]	Prevent vampire attacks through routing protocol	Detection through behavior analysis

TABLE II

BEHAVIOR TABLE

Parameters	Normal	Abnormal			
		Vampire	U2R	Probe	DoS
Packet Type	TCP, UDP, AODV	Energy = 0	IP modification	Loop	Message
Event Type	S, R, F	D	R, D	D	F
Acknowledgement	Yes	No	No	No	No
Queue Utilization	N	H	H	H	H

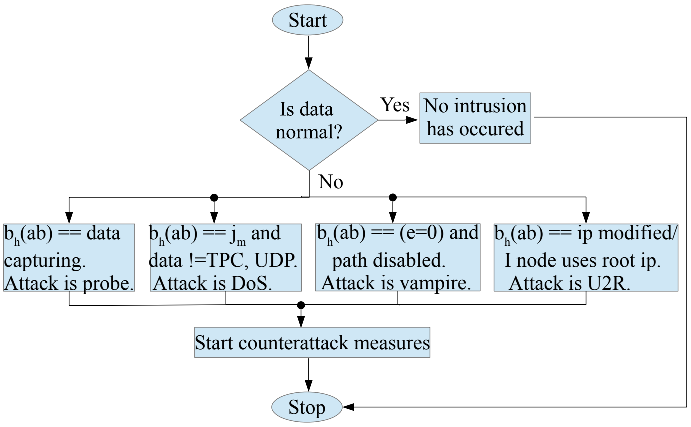

Start
Is data normal?
Yes
No intrusion has occured
No
b_h(ab) == data capturing. Attack is probe.
b_h(ab) == j_m and data !=TPC, UDP. Attack is DoS.
b_h(ab) == (e=0) and path disabled. Attack is vampire.
b_h(ab) == ip modified/ I node uses root ip. Attack is U2R.
Start counterattack measures
Stop

Fig. 2. Flowchart for proposed algorithm

TABLE III

NETWORK SIMULATION PARAMETERS

Parameter	Value
Number of nodes	50
Simulation area	800 × 800 m
Routing Protocol	AODV
Attack types	Probing, DoS, vampire, U2R
Simulation time	100 seconds
Transport layer	TCP, UDP
Traffic type	CBR, FTP
Packet size	512 bytes
Mac Standard	802.11
Antenna type	Omni-Antenna
Number of Traffic connections	10
Node speed	Random

utilization is high which proves there are more malicious nodes in the queue.

The parameters considered for network modeling are number of nodes, simulation area, standard routing protocol type, transport protocol, MAC standards, application protocols and antenna type as shown in Table III. All these parameters are useful for network architecture design and analyzing the behavior of the MANET.

IV. NETWORK OUTPUT RESPONSES

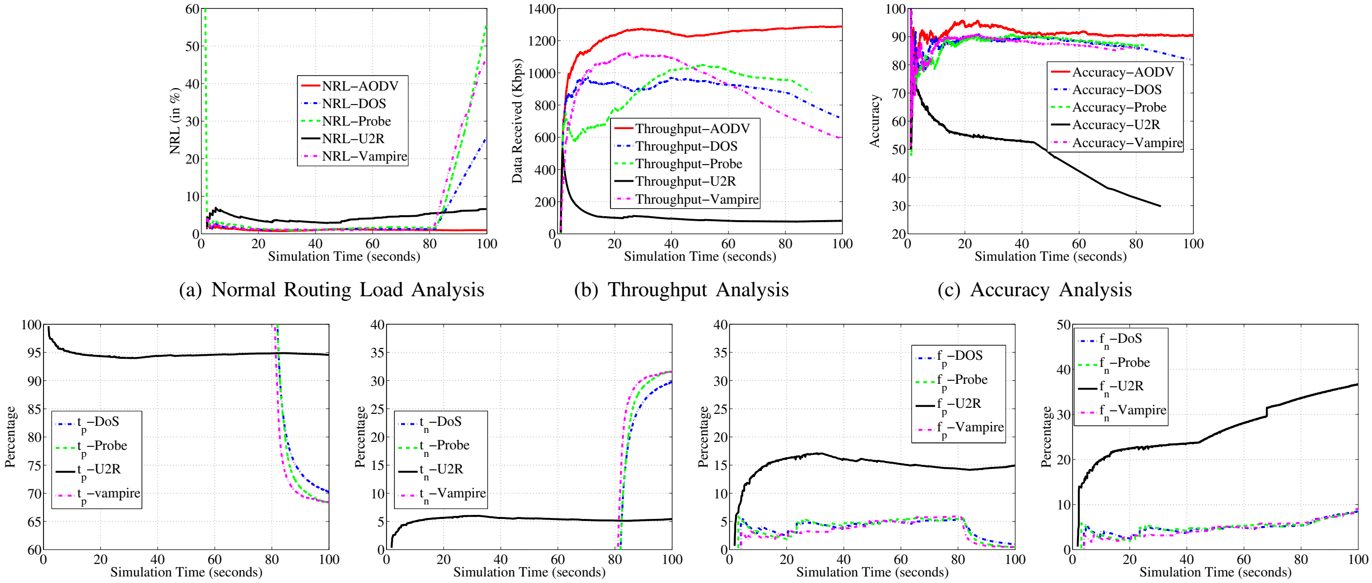
This section describes the response of the simulated network under normal conditions (no attack) as well as abnormal conditions (under attack). The responses reported are Throughput, Normal Routing Load (NRL), End-to-End Delay, Accuracy, Confusion Matrix i.e. True positives (t_p), True negatives (t_n), False positives (f_p), False negatives (f_n). For each output response, we compare the behaviour of AODV routing under no attack with AODV routing under DoS attack, probing attack, U2R attack and vampire attack. So, for each output response, there are 5 different scenarios.

A. Normal Routing Load

Normal routing load (NRL) is the ratio between number of routing packets (N_{rpkt}) to the total data received by the receivers ($Data_{received}$), as shown in equation 1.

$$NRL = \frac{N_{rpkt}}{Data_{received}} \times 100. \tag{1}$$

When the ratio is minimum it means network overhead is low. We report that AODV routing under normal conditions requires low overhead and U2R attack requires 8% more overhead because U2R gives wrong route frequently in order to lower the requirement of routing packets in this scenario. The other three attacks spread junk packets in the network so the network is heavily congested and thus increase the



(a) Normal Routing Load Analysis

(b) Throughput Analysis

(c) Accuracy Analysis

(d) True Positive Analysis

(e) True Negative Analysis

(f) False Positive Analysis

(g) False Negative Analysis

Fig. 3. Network Output Responses.

overhead of the network. Figure 3(a) shows the NRL in the 5 different scenarios where x-axis shows the simulation time in seconds and y-axis shows the NRL (in %).

B. Throughput Analysis

Figure 3(b) shows the throughput for 5 different cases where x-axis shows the simulation time in seconds and y-axis shows the data received per second (Kbps). Throughput is defined as the ratio between data received by the receivers (Data$_{received}$) and Time (in seconds) as shown in equation 2.

$$Throughput = \frac{Data_{received}}{Time(sec.)}. \qquad (2)$$

AODV distance vector routing in no attack environment provides higher throughput, whereas the 4 scenarios under attack environment capture the genuine data through attacker nodes and decrease the throughput of the network. For the probing attack scenario, the throughput is 0 from 90th second onwards, meaning no data is received by the genuine receiver, all the data is received by the attacker resulting in damage to the whole network.

C. Accuracy Analysis

Accuracy in terms of network communication is the percentage of accurate data received by the receivers. When the attacks are not present in the network its performance is better. Figure 3(c) shows that all 4 types of attacks degrade the network performance, because each attacker module modifies the data packets and corrupt it. This corrupt data is treated as inadequate data. In the case of U2R attack, the accuracy degrades from 70% to 30% implying that U2R attack is more harmful than other attacks. AODV routing under no attack shows above 90% accuracy in receiving data.

D. End-to-End Delay Analysis

End to end delay depends on various factors of the network i.e. congestion status, queue, utilization, number of available paths and channel capacity. From Table IV, we observe that AODV under normal conditions generates minimum delay for data transmission and in other 4 cases, when the network is under attack, the end-to-end delay increases because unwanted junk messages are transmitted by the attacker node that increase the network delay from the unnecessary queue and bandwidth utilization.

TABLE IV
AVERAGE END-TO-END DELAY

Network	End-to-End Delay (ms)
Normal	0.33
DoS	0.52
Vampire	0.45
Probe	0.52
U2R	0.65

E. True Positive analysis

True positive is the total set of normal data (TCP, UDP) which are detected by the detection algorithm. When the transmitted data is passed through the detection algorithm, the data is compared with the respective format of particular data and if it is 100% accurate, it means it is true positive data. In Figure 3(d), DoS attack, probing, U2R and vampire attack are considered for the analysis and it is observed that for U2R the true positive is nearly 95%. However, for the other 3 cases true positive is 100% till 80 seconds and after that result degrades because the nodes move out of the radio zone.

Algorithm 1 Intrusion Detection Algorithm

```
Input Factors:
M: Mobile node, S: Source node, R: Receiver node, $\Psi$ : Radio range = 550m, $b_h$(n,ab): behavior table containing normal and abnormal behaviors, I: Set of intermediate nodes, A: Attack types (probing, vampire, DoS, U2R), $j_m$: Junk message, e: Energy of nodes, $R_p$: AODV routing protocol, rpkt: Routing Packet
Output Responses: Throughput, Normal Routing Load (NRL), End-to-End Delay, Accuracy, Confusion Matrix i.e. True positives ($t_p$), True negatives ($t_n$), False positives ($f_p$), False negatives ($f_n$).
Procedure:
S $\leftarrow$ broadcast (AODV, S, R)
if I $\neq$ R and I in $\Psi$ then
    I $\leftarrow$ receive rpkt
    I $\leftarrow$ forward rpkt to next hop
else if I == R then
    R $\leftarrow$ receives rpkt
    Select shortest path
    R $\leftarrow$ create reverse route for ack
    S $\leftarrow$ receives ack
    Send data (S, R, data)
else
    Node out of range
    Node unreachable
end if
Attack detection module:
Data passes into detection engine, Compare data and $b_h$(n,ab).
if data == $b_h$(n) then
    data is normal TCP, UDP or AODV
else if data ==$b_h$(ab) then
    Data shows abnormal activity: A
    if $b_h$(ab) == data capturing then
        A $\leftarrow$ probe
    else if $b_h$(ab) == $j_m$ and data $\neq$ TCP, UDP, AODV then
        A $\leftarrow$ DoS
    else if $b_h$(ab) == (e=0) and path disabled then
        A $\leftarrow$ vampire
    else if $b_h$(ab) == ip modified or I node uses root ip then
        A $\leftarrow$ U2R
    end if
end if
```

F. True Negative analysis

True negative is the total set of abnormal data which is detected by detection algorithm. If the data detected does not belong to the actual data group it means the data is abnormal and based on abnormality it can be classified as a particular attack. When the attacker node retrieves credentials of normal user and gains access to the root node, it signifies that it is a U2R attack. Similarly, if a node consumes network energy and degrades the network actual performance, then it is a vampire attack. In Figure 3(e), the true negative is shown for 4 attack scenarios.

G. False Positive Analysis

False positive also known as false alarm, is the total set of normal data which are detected but should actually be abnormal data. If the value is low or zero, it signifies that the proposed detection algorithm is accurate in measuring the abnormality. In the data transmission some data properties are depicted as normal data but they are actually unusual data which are not detected under true negative. All this data belongs to the category of false positive that creates confusion for detection algorithm. In Figure 3(f), all 4 types of attack are analyzed under MANET environment. The percentage is not greater than 20% meaning that a maximum 20% confusion for attack is detected from detection algorithm.

H. False Negative Analysis

False negative is the total number of abnormal instances detected which should be normal data. That abnormality in network is due to some reason i.e. either some packet has been dropped by the MAC, collision, route or queue based drop. However, the system detects the dropped data as attack symptoms and the data is treated as unusual by the detection algorithm. In Figure 3(g), all four type of attacks are measured.

The overall performance summary is presented in Table V.

TABLE V
PERFORMANCE SUMMARY

Parameter (units)	DoS	Vampire	Probe	U2R	Normal
SEND (no. of packets)	5142	3901	4756	1586	8238
RECV (no. of packets)	4196	3203	3901	423	7458
PDF (% data received)	81.6	82.11	82.02	26.67	90.53
NRL	25.91	46.99	56.42	6.82	1.01
End-to-End Delay (ms)	0.52	0.45	0.52	0.65	0.33
Dropped packets (no. of packets)	946	698	855	1163	780

V. CONCLUSIONS AND FUTURE RESEARCH

In this paper we have presented an intrusion detection algorithm to detect the probing, vampire, DoS and U2R attacks. We have shown that all the four type of attacks degrade the network performance with respect to throughput, accuracy, NRL and End-to-end delay. We have shown the efficiency and accuracy of our proposed algorithm using confusion matrix. True positive gives the minimum output nearly 70% implying that 70% is truly detected normal data by detection algorithm. Other analysis (True negatives, False positives, False negatives) also show promising results. For future research, this work will be extended for prevention of detected attacks through lightweight techniques. Also, the algorithm may be revised to handle multiple types of attacks occurring simultaneously in the network.

References

[1] S. E. Khediri, N. Nasri, A. Benfradj, A. Kachouri, and A. Wei, "Routing protocols in MANET: Performance comparison of AODV, DSR and DSDV protocols using NS2," in *Proceedings of the IEEE International Symposium on Networks, Computers and Communications*, 2014, pp. 1–4.

[2] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and U. Choppali, "Wireless Sensor Network Simulation Frameworks: A Tutorial Review," *IEEE Consumer Electronics Magazine (CEM)*, vol. 6, no. 2, pp. 63–69, April 2016.

[3] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[4] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008.

[5] S. Ganapathy, P. Yogesh, and A. Kannan, "An intelligent intrusion detection system for mobile ad-hoc networks using classification techniques," *Communications in Computer and Information Science*, vol. 148, pp. 117–122, 2011.

[6] S. R. Das, E. M. Belding-Royer, and C. E. Perkins, "Ad hoc on-demand distance vector (aodv) routing," 2003.

[7] Al-Yaseen, W. Laftah, Z. A. Othman, and M. Z. A. Nazri, "Real-time intrusion detection system using multi-agent system," *IAENG International Journal of Computer Science*, vol. 43, no. 1, pp. 80–90, 2016.

[8] S. Paliwal and R. Gupta, "Denial-of-service, probing and remote to user (r2l) attack detection using genetic algorithm," *International Journal of Computer Applications*, vol. 60, no. 19, pp. 57–62, 2012.

[9] J. Sen, "A distributed intrusion detection system using cooperating agents," *arXiv preprint arXiv:1111.0382*, 2011.

[10] S. T. Sheu, M. Kao, Y. Hsu, and Y. en Cheng, "Secure routing protocol for detecting grayhole attack and false report along with elliptic curve cryptography in wireless sensor network," in *Proceedings of the IEEE Students Conference on Electrical, Electronics and Computer Science*, 2014.

[11] A. Vincy and V. U. Devi, "Maximizing lifetime of nodes in wireless ad hoc sensor network by preventing vampire attack," in *Proceedings of the IEEE International Conference on Innovations in Engineering and Technology*, 2014.

[12] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *IEEE transactions on vehicular technology*, vol. 58, no. 1, pp. 367–380, 2009.

[13] S. Doshi, S. Bhandare, and T. X. Brown, "An on-demand minimum energy routing protocol for a wireless ad hoc network," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 50–66, 2002.

[14] S. S. George and R. Suma, "Attack-resistant routing for wireless ad hoc networks," *International Journal of CS & IT*, vol. 5, no. 3, 2014.

[15] S. Bose and A. Kannan, "Detecting denial of service attacks using cross layer based intrusion detection system in wireless ad hoc networks," in *Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking*, 2008, pp. 182–188.