



# Anomaly Intrusion detection system in Network based MANET's

<sup>1</sup>Mohammed Shabaz Hussain, <sup>2</sup>Khaleel Ur Rahman Khan

<sup>1</sup>Research Scholar (PP.COMP.SCI.0531), Department of Computer Science, Rayalseema University, Kunool, A.P, India

<sup>2</sup>Professor, department of Computer Science and Engineering, ACE Engineering college, Medchal, District, Ghatkesar, India.

## Abstract :

In the communication model of wired and wireless Adhoc networks, the most needed requirement is the integration of security. Mobile Adhoc networks are more aroused with the attacks compared to the wired environment. Subsequently, the characteristics of Mobile Adhoc networks are also influenced by the vulnerability. The pre-existing unfolding solutions are been obtained for infrastructure-less networks. However, these solutions are not always necessarily suitable for wireless networks. Further, the framework of wireless Adhoc networks has uncommon vulnerabilities and due to this behavior it is not protected by the same solutions, therefore the detection mechanism of intrusion is combinedly used to protect the Manets. Several intrusion detection techniques that have been developed for a fixed wired network cannot be applied in this new environment. Furthermore,

The issue of intensity in terms of energy is of a major kind due to which the life of the working battery is very limited. The objective this research work is to detect the Anomalous behavior of nodes in Manet's and Experimental analysis is done by making use of Network Simulator-2 to do the comparative analysis for the existing algorithm, we enhanced the previous algorithm in order to improve the Energy efficiency and results shown the improvement of energy of battery life and Throughput is checked with respect to simulation of test case analysis.

**Keywords—** Intrusion detection system, Network Protocols, Wireless Network, component, IDS

## 1. Introduction.

The communication of various nodes present in a wireless network environment is done without any support of any centric behavioral node or coordinator, therefore any intended node determined or aimed to communicate then it is done with the intermediary node which is present in the range of communication of passing the information or message. The dynamic delineation of the network may change due to the movement of nodes and in turn, causes to intervene of new other nodes in the network and formation of such nodes is easily structured and dismounts or deprive

The challenging task of MANET is due to flexible characteristics and loss of centralized control of infrastructure-less nodes with high-security risk and lack of wireless communication link The security in the wireless medium is provided by introducing the mechanism of intrusion detection techniques. The detection of unintended activity in wireless nodes is identified with different mechanisms of intrusion detection techniques, The intrusions are broadly divided into four categories as Signature-based IDS, Anomaly-based IDS, Network-based IDS, and Host-based IDS. The signature-based IDS is used for detecting the known patterns of intrusions, Anomaly-based IDS is used for detecting the dropping of any data packet, Network-based IDS is used for analyzing the data in a network of huge traffic. The Host-based IDS is used for detecting the attacks in the operating system and log files of the system.[1],[2],[30]. The challenge of making the less battery power usage due to high data processing and gauging of IDS will turn as an outlay of cost burden. Thus this causes how to make usage of IDS for a minimum time without a drop of its effectiveness is the basic requirement.

## 2. Related Work.

In [7], Dong et al. has done the study to enhance the topology of the network in order to obtain the monitoring concept with maximizing the network lifetime in an efficient approach, To this optimized selection of node is done to monitor the nodes rather than keeping all the nodes to monitoring purpose to improve the energy level. A node selected as a monitor node will be treated as an active node that tolerates the monitoring of all other nodes in the network when the other nodes are under a sleep mode. With this energy consumption is obtained in overall behavior characteristics. In SLAM [8], SLAM protocol maintains the guard node to monitor any malicious behavior in the network, based on the Trust value. If the node trust value is above the Trust then it will activate the agent of detecting intrusion activity in the network [9]. The Energy saving level can be maximized by putting all the other nodes present in the network into a sleep mode. There are broadly divided into three categories. The first category is known as scheduling of sleep synchronized wakeup-sleep, here the nodes of the network are put in a sleep mode and behave in two ways as distributed or another as centralized manner when nodes are woken-up [10][11][12] [13].

The second category is referred to like the selection of the subset of nodes which are to be woken-up and maintains the property of sensing and network connectivity or both are included [14][15][16]. The third category is referred to as a mechanisms protocol called a sleep-wake-up based on-demand [17][18]. According to the researcher R. Rodrigo's work was discussed is for developing an efficient IDS for mobile ad-hoc networks but these are developed for the prevention of attacks with different techniques [19],[20],[21],[22]. Currently, the prevention techniques and IDS in wireless sensor networks are developed in a trusted environment [23], [24],[25],[26-32].

## 2. Problem Statement.

### 2.1 Problem Definition

The existing system consists of nodes that maintain IDS with each of the nodes and monitors malicious behavior. As battery power is limited this causes loss of battery energy due to all the time usage of battery power with each of the nodes to overcome this drawback a protocol named as SLAM protocol is used which maintains guard node within the network whose activity is to monitor the nodes locally and the Threshold is maintained to detect the malicious node in the network the Threshold is the malicious counter notating as a malicious (p,q). When a Threshold value of a node has crossed the limit then such a node is referred to as a malicious node.[1]

### 2.1 Problem Solution.

In the proposed system the usage of battery is prevented due to its continuous active time duration of IDS therefore when any node of IDS is not in use then such node will be in an inactive state and this reduces energy consumption in Manet's [31]. The selection of making the nodes in an active and inactive state is implemented by applying the level of Security designated to m nodes from a total of n nodes, to detect the unintended anomalous behavior, The secondary goal of my work is to reduce the energy level compared to the existing energy obtained previous security levels,

## 3. IDS Architecture

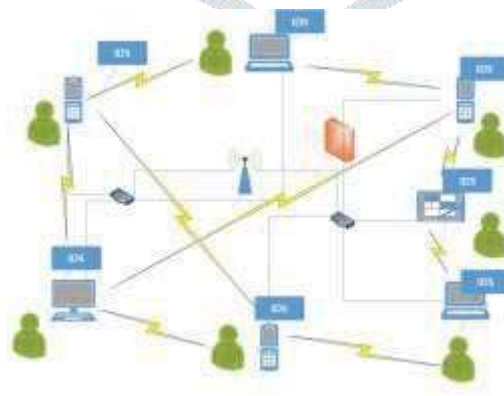


Figure 1 : IDS Architecture

Figure 1, Represents The working of IDS Architecture consists of 'n' number of nodes (computer), in each of these nodes IDS is installed, among these nodes, the enhanced Mdk algorithm is embedded within the IDS in order to identify the anomalous behavior among the nodes. Then, the node(s) in which IDS is installed will determine the minimum probability with which it has to monitor its neighborhood traffic within the network and starts collecting the information from the neighboring nodes by sending the message request to those node(s) which has one-hop distance in the network. The Security of the nodes is maintained by finding the degree information from all the nodes and whose node degree is less, that specific node is chosen and compared with their subsequent degree nodes. Then, the node that has minimal degree will be assigned as a basis for providing the security level in the network. For example, if the Degree level is 2,4,5,6 the minimum degree value node will be considered as the security level and those numbers of nodes will be activated and with this few nodes and remaining nodes will be in the inactive state. Thus, this approach reduces the power usage of the battery [5],[6].

To illustrate the comparative analysis is done by using the NS-2 simulator by performing various operations such as sending of packets between the set of nodes and it has been observed that the usage of energy by each of these nodes is reduced. The comparison between the existing and proposed systems is done by using various performance metrics such as throughput and energy consumption as shown below in the tables and graphs.

#### 4. The performance metric for Throughput

The probability of the neighbors is calculated and compared with the threshold value. Here, the security level has been taken as the threshold value given below [1].

$$\text{Probability}(p) = \text{Security level} / \text{No. of neighbors}$$

Security Level is the number of neighbor monitoring a node at any instant of time. It means a node is monitored by at least 1 of its neighbors at any instant of time

#### 5. The performance metric for Energy consumption

The energy consumption for the proposed MDK algorithm in IDS is tested using the following equation [1].

$$\begin{aligned} \text{Energy} &= \text{initial energy} - \text{final energy} \\ \text{Energy (joules)} &= \text{Power (Watts)} * \text{Time (sec)} \end{aligned}$$

#### 6. ALGORITHM MDK

Input: Nodes and messages Output: Degrees Selective nodeBegin :

1. Respond to each node of M with Know degree and Reply message.
2. Know degree and Reply message is responded by each node of M
3. do for each message,
4. Each node individually sends a message to all the other nodes to know their degree to each of the nodes.
5. M -> Transmit ( Know Degree )
6. On Receiving the KnowDegree message each of the nodes responds to every other node say for N by replying message of their degree.
7. Degree = KnowDegree
8. The Security Level say as S then  $S > K$ , Then  $K = \text{Minimal ( degree )}$
9. If  $S > K$  then the Probability  $\text{Probmin} = 1$ , Probability minimum value is assigned.
10. END

## 7. Algorithm steps for minimal degree calculation

The MDK algorithm shown in Figure 2, calculates the minimal degree of each of the nodes say for 'M' with the probability through which intense it monitors the neighboring nodes.

- i. In Step 1, M transmits the message to find the Knowndegree,
- ii. In Step 2 to step 5, all the other nodes present as neighbors reply with its neighboring degree.
- iii. Step 6 receives the degree of all its neighboring nodes assigned with some probability.
- iv. In Step 7 The algorithm accepts a lower degree of their network nodes, whereas and does not accept the message whose degree is high
- v. In step 8 The Degree of whose node is high is treated as a malicious node.

## 8. Results Analysis

For the simulation, the following constants are considered as shown in Figure 2.

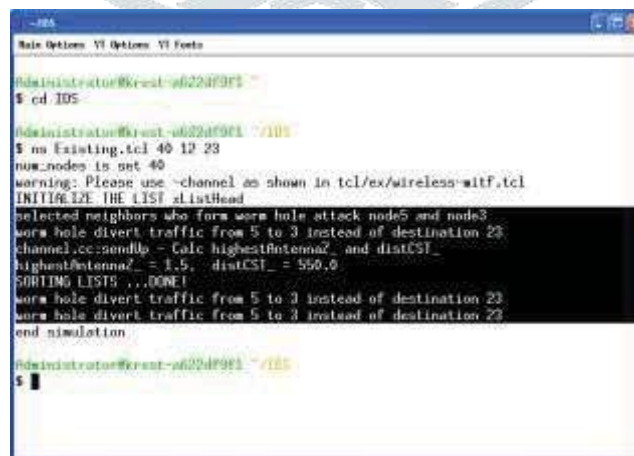


```

Administrator@Kreat-a622d9f1:~$ cd IOS
Administrator@Kreat-a622d9f1:~/IOS$ ns Existing.tcl 40 12 23
  
```

Figure 2. Shows Nodes 40,12 and 13

In the above Figure 2, by using the command we are running an existing simulation technique in which 40 is total no of nodes and 12 is the source node and 23 is the destination node. After running the above command will get below result on the screen.



```

Administrator@Kreat-a622d9f1:~$ cd IOS
Administrator@Kreat-a622d9f1:~/IOS$ ns Existing.tcl 40 12 23
warning: Please use -channel as shown in tcl/ex/wireless-wtf.tcl
INITIALIZE THE LIST alisthead
selected neighbors who form worm hole attack node5 and node3
worm hole divert traffic from 5 to 3 instead of destination 23
channel_ccsendlls - Calc highestAntenna2_ and distCSI_
highestAntenna2_ = 1.5, distCSI_ = 550.0
SORTING LISTS ...DONE!
worm hole divert traffic from 5 to 3 instead of destination 23
worm hole divert traffic from 5 to 3 instead of destination 23
end simulation
Administrator@Kreat-a622d9f1:~$
  
```

Figure 3. Selection of any two nodes as a Blackhole attack

In above Figure 3, any two nodes are made as a malicious node; here node 3 and 5 are deployed as a malicious node. The outputs are depicted in Figure 5 after the creation of 40 nodes. Figure 6, shows the malicious nodes and the sending of packets from node 3 to node 6.

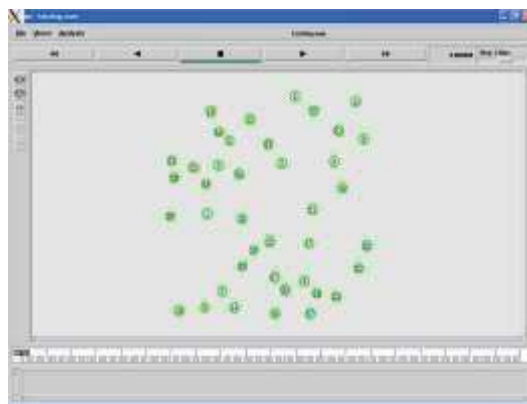


Figure 4. Creation 40 nodes

TABLE I. SIMULATION PARAMETER DESCRIPTION

Simulation time	200s	Max Speed	25 m/s
Area	1000x 1000m	Packet Rate	4pkt/sec
Number of Mobile Hosts	20,50	Pause Time	0 sec



Figure 5. Route Discovery Phase of packets

```

Admin@star@root-622d7911 ~$ ns
ns: ns 1.0M.tcl 40 12 25
now nodes is set 40
warning: Please use -channel as shown in tcl/ex/wireless-wire.tcl
Please enter security level
?
INITIALIZE THE LIST $listhead
node12 use hop neighbors : 2 3 5 11 15 25 36 38
Monitoring probability for source 12 is : 4.4444444444444446
Monitoring probability for first neighbor 5 is : 1.1111111111111112
Monitoring probability for second neighbor 3 is : 1.1111111111111112
Selected neighbors who form worm hole attack nodes and nodes
worm hole divert traffic from 5 to 3 instead of destination 23
channel::modify - Calc highestAntenna2_ and distCSI_
highestAntenna2_ = 1.5; distCSI_ = 550.0;
SORTING LISTS ...DONE!
worm hole divert traffic from 5 to 3 instead of destination 23
worm hole divert traffic from 5 to 3 instead of destination 23
end simulation
Admin@star@root-622d7911 ~$
    
```

Figure 6. System is asking for security level and security level value entered.

The security level is calculated to determine the one hop monitoring probability to detect the worm hole attack,





The Throughput, with respect to existing and proposed, is shown in Figure 13.

TABLE II. SIMULATION PARAMETER DESCRIPTION

Time (m/s)	Throughput Existing system	Throughput enhanced MDk
3	335.710206	395.34488
4.000922	748.796496	919.9977315
5.008584	1171.104144	1486.003254
6.00178	1594.052992	2223.900386
7.005924	2017.399916	3046.145829

The comparative analysis of throughput of the proposed approach is high compare to the existing system is shown in Table II.

### Test Case 1

Total numbers of Nodes – 20

The following graph shows the energy consumed by the nodes at different security levels

TABLE III. ENERGY VALUES TOTAL OF 20 NODES

Security Level	Energy consumption (existing approach)	Energy consumption (Proposed approach)
1	2946.3	1151.25
2	2933.07	993.194
3	2901.8	1114.2
4	3000	1167.59
5	2946.3	1159.71

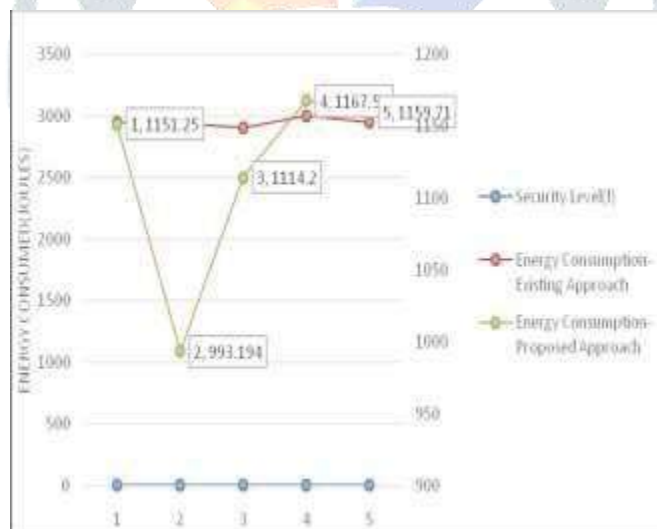


Figure 13 : Energy graph for Test Case 1



**Test Case -2**

TABLE IV. TOTAL NUMBER OF NODES ACTIVE- 30

Security Level	Energy consumption (existing approach)	Energy consumption (Proposed approach)
1	2860.75	1087.83
2	2934	1141.73
3	2884.68	1137.3
4	2914.91	1160.93
5	2903.11	1115.62

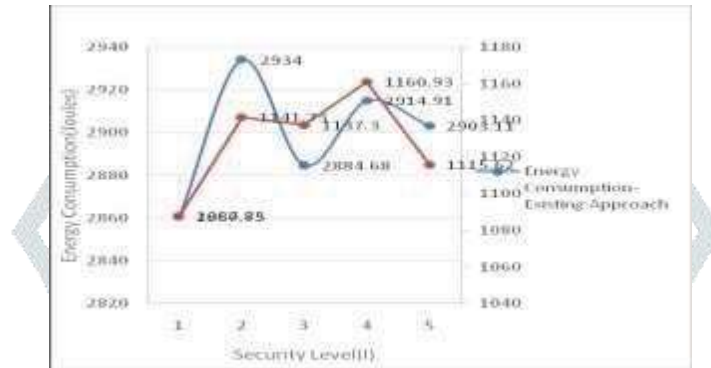


Figure 14 : Energy Consumption graph

**9. Conclusion**

This research concludes that the energy consumption is reduced and battery life is increased exponentially when compared with the existing approach by using an ns-2 simulator as shown in Table III. Further, the test cases are shown in Figure 14 and Figure 15. In the future, we plan to enhance the proposed approach by using classification algorithms of Data mining such as J48.

**11. References**

- [1] A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks Ningrinla Marchang, Member, IEEE, Raja Datta, Senior Member, IEEE, and Sajal K. Das, Fellow, IEEE
- [2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.
- [3] S. K. Bhoi and P. M. Khilar, "Vehicular communication: A survey," *IET Netw.*, vol. 3, no. 3, pp. 204–217, 2014.
- [4] S. Marti, T. J. Giuli, K. La, and M. Baker, "Mitigating routing misbehavior in a mobile ad-hoc environment," in *Proc. 6th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw.*, pp. 255–265, 2000.
- [5] C. Manikopoulos and L. Ling, "Architecture of the Mobile Ad-hoc Network Security (MANS) system," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2003, vol. 4, pp. 3122–3127.
- [6] K. Nadkarni and A. Mishra, "Intrusion detection in MANETs—The second wall of defense," in *Proc. IEEE Ind. Electron. Soc. Conf.*, Roanoke, VA, USA, Nov. 2–6, 2003, pp. 1235–1239.
- [7] D. Dong, X. Liao, Y. Liu, C. Shen, and X. Wang, "Edge self-monitoring for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 514–527, Mar. 2011.
- [8] I. Khalil, S. Bagchi, and N. B. Shroff, "SLAM: Sleep-wake aware local monitoring in sensor networks," in *Proc. 37th Annu. IEEE/IFIP Int. Conf. DSN*, 2007, pp. 565–574.
- [9] T. Hoang Hai and E.-N. Huh, "Optimal selection and activation of intrusion detection agents for wireless sensor networks," in *Proc. IEEE FGNC*, Dec. 6–8, 2007, vol. 1, pp. 350–355.

- [10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," in *Wireless Networks*, vol. 3 (5), pp. 48 - 494, 2002
- [11] S. Bhattacharya, G. Xing, C. Lu, G.-C. Roman, O. Chipara, and B. Harris, "Dynamic wake-up and topology maintenance protocols with spatiotemporal guarantees," in the fourth workshop on Information Processing for Sensor Networks (IPSN), pp. 28-34, 2005.
- [12] S. Kumar, T. H. Lai, and J. Balogh, "On k-coverage in a mostly sleeping sensor network" in the ACM Intl. Conference on Mobile Computing and Networking (MOBICOM), pp. 144-158, 2004
- [13] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy- Efficient Communication Protocol for Wireless Microsensor Networks," in the 33rd Hawaii Intl. Conference on System Sciences (HICSS), pp. 3005-3014, 2004.
- [14] G. Xing, X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration for energy conservation in sensor networks," in *ACM Trans. on Sensor Networks (TOSN)*, Vol. 1 , Issue 1, pp. 36-72, 2005
- [15] T Singh, J Singh, S Sharma, "Energy efficient secured routing protocol for MANETs", *Wireless Networks*, Springer, 2017.
- [16] R. Naik, S. Biswas, and S. Datta, "Distributed SleepScheduling Protocols for Energy Conservation in Wireless Networks," in the 38th HICSS, pp. 285b - 285b, 2005.
- [17] C. Guo, L. C. Zhong, and J. M. Rabaey, "Low power distributed MAC for ad hoc sensor radio networks," in *IEEE Global Telecommunications Conference (GLOBECOM '01)*, pp. 2944–2948, vol.5, 2001.
- [18] [http://www.austriamicrosystems.com/03products/data/AS3931Product\\_brief\\_0204.pdf](http://www.austriamicrosystems.com/03products/data/AS3931Product_brief_0204.pdf). (online).
- [19] Roman, R.; Jianying Zhou and Lopez, J. Applying intrusion detection systems to wireless sensor networks, 3rd IEEE Consumer Communications and Networking Conference, 2006.
- [20] P Pandey, A Barve, "An Energy-Efficient Intrusion Detection System for MANET", *Data, Engineering and Applications*, Springer, 2019.
- [21] Santos, L., Rabadao, C., & Goncalves, R. "Intrusion detection systems in Internet of Things: A literature review", 13th Iberian Conference on Information Systems and Technologies (CISTI), 2018
- [22] Doumit, S. and Agrawal, D. P. Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network, *IEEE Military Communications Conference, MILCOM 2003*
- [23] Onat, I. and Miri, A. An Intrusion Detection System for Wireless Sensor Networks, *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, 2005.
- [24] Banerjee, S.; Grosan, C. and Abraham, A. IDEAS: intrusion detection based on emotional ants for sensors", 5th International Conference on Intelligent Systems Design and Applications, 2005.
- [25] Techateerawat, P. and Jennings, A. "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks", *IEEE/WIC/ACM International Conference on Web Intelligence and International Agent Technology Workshops*, 2006.
- [26] A. P. R. Da Silva; A. A. F. Loureiro; M. H. T. Martins; L. B. Ruiz; B.P. S. Rocha and H. C. Wong. "Decentralized Intrusion Detection in Wireless Sensor Networks", *International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, October 2005.
- [27] Chong, E. L.; Mun, Y. N.; Christopher, L. and Marimuthu, P. "Intrusion Detection for Routing Attacks in Sensor Networks", *International Journal of Distributed Sensor Networks*, Vol. 2, n. 4, October – December, 2006.
- [28] Weichao, W. and Bharat, B. Visualization of "Wormholes in Sensor Networks, In Proceeding of the 2004 ACM workshop on wireless security", 2004.
- [29] Khalil, I.; Saurabh Bagchi and Shroff, N.B. "LITEWOP: a lightweight countermeasure for the wormhole attack in multihop wireless networks", In *Proceeding of International Conference on Dependable Systems and Networks*, 2005.
- [30] M Liu, Z Xue, X Xu, C Zhong, J Chen, "Host-based intrusion detection system with system calls: Review and future trends" *ACM Computing Surveys (CSUR)*, 2019.
- [31] Praveena, A., and S. Smys. "Anonymization in social networks: a survey on the issues of data privacy in social network sites." *Journal of International Journal Of Engineering And Computer Science* 5, no.3 (2016): 15912-15918.
- [32] A Keshavarzian, C Peters, M Bocca, "Energy Efficient Intrusion Detection System", *Google US Patent App. 16/066,575*, 2019