Latency and Power Aware Reliable Intrusion Detection System for Ensuring Network Security in Military Applications

L. Sheeba, V.S. Meenakshi

Abstract--- Intrusion detection system is a most concerned research area which needs to be detected earlier to avoid the unwanted network errors and problems. The accurate and reliable intrusion detection is a most focused research problem in various domains which is found to be more difficult issue. This is focused and resolved in the previous research work namely Prioritization Based Delay Avoided Secured and Reliable Data Transmission Method (PBDASRDT). However, this research method doesn't focus on the energy conservation parameters. And also previous work doesn't discuss about the security provisioning methods. This is focused and resolved in this research method by introducing the method namely Latency and Power aware Reliable Intrusion Detection System (LP-RIDS). In this research method latency and power consumption of servers in which intrusion detection is performed is reduced considerably by introducing the secondary cluster head selection process. This secondary cluster head can perform the energy management of IDS servers optimally between the nodes and gateway. And then security of the intrusion detection system is enhanced by introducing the dynamic key based encryption technique. Here the dynamic key generation process is done in the secondary cluster head and the encryption is done by using AES technique. This methodology can improve the network performance considerably by detecting the attacks more accurately with reduced latency and delay. The overall evaluation of the research method is done in the NS2 simulation environment from which it is proved that the proposed research method leads to ensure the enhanced outcome than the existing research methods. This method proved to provide the protection from the denial of service attacks in the efficient way, thus ensuring security with reduced computational cost.

Keywords--- Secured Data Transmission, Intrusion Detection, Latency and Power Reduction, Secondary Cluster Head, Dynamic Key Generation, Encryption.

I. INTRODUCTION

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an Intrusion Detection System (IDS) is a system for the detection of such intrusions [1]. Since prevention techniques cannot be sufficient and new intrusions continually emerge, IDS is an indispensable part of a security system [2]. An IDS is introduced to detect possible violations of a security policy by monitoring system activities and responding to those that seem intrusive [3]. If we detect the attack once it comes into the network, a response can be initiated to prevent or minimize the damage to the system. An IDS also helps prevention techniques improve by providing information about intrusion techniques [4].

There have been many approaches proposed for intrusion detection. Intrusion detection methods are classified into three main techniques: anomaly-based, misuse-based, and specification-based [5].

An anomaly-based technique profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs and so on. It detects intrusions as anomalies, i.e. deviations from the normal behaviors [6]. In the literature, various techniques have been applied for anomaly detection, e.g. statistical approaches, and artificial intelligence techniques like data mining and neural networks. Misuse-based detection compares known attack signatures with current system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate [7]. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, these techniques are generally employed together for effective intrusion detection. Specification-based technique is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with lower false positive rate [8]. In this technique, a set of constraints of a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. Most host-based Intrusion Detection Prevention Systems (IDPS) can detect several types of malicious activity [9]. They often use a combination of signature-based detection techniques to identify known attacks, and anomaly based detection techniques with policies or rule sets to identify previously unknown attacks. The types of events detected by host-based IDPSs vary considerably based primarily on the detection techniques that they use. Some host-based IDPS products offer several of these detection techniques, while others focus on a few or one [10]. In this research method latency and power consumption of servers in which intrusion detection is performed is reduced considerably by introducing the secondary cluster head selection process.

II. RELATED WORKS

Panda et. al. [11], compares different data mining techniques for intrusion detection system and found that accuracy & performance of Naïve bayes classifier for all classes is better than the accuracy obtained in the case of

Manuscript received September 16, 2019.

L. Sheeba, Research Scholar, Bharathiyar University, Coimbatore. T.N, India.(e-mail: Sheebcom@gmail.com)

Dr.V.S. Meenakshi,Assitant Professor, Chikkena Government Arts College, Trippur. T.N, India. (e-mail: meenasri 07@gmail.com)

different Decision tree algorithm but Decision tree is robust in detecting unknown intrusions in comparison to Naïve bayes classification algorithm.

Ektela et.al. [12] presented Support Vector Machine and classification tree Data mining technique for intrusion detection in network. They compared C4.5 and Support Vector Machine by experimental result and found that C4.5 algorithm has better performance in term of detection rate and false alarm rate than SVM, but for U2R attack SVM performs better.

Hu et.al [13] presented fast machine-learning-based intrusion detection algorithms with high detection rates and low false-alarm rates. In the algorithm, decision stumps are used as weak classifiers.

The decision rules are provided for both categorical and continuous features. By combining the weak classifiers for continuous features and the weak classifiers for categorical features into a strong classifier, the relations between these two different types of features are handled naturally, without any forced conversions between continuous and categorical features.

Adaptable initial weights and a simple strategy for avoiding over fitting are adopted to improve the performance of the algorithm.

Gao et.al [14] presented distributed IDS framework. It consists of the individual and global models. Specifically, the individual model for the local unit derives from Gaussian Mixture Model based on online Adaboost algorithm, while the global model is constructed through the PSO-SVM fusion algorithm.

Experimental results demonstrate that our approach can achieve a good detection performance while being trained online and consuming little traffic to communicate between local units.

Yang et.al [15] presented new Firefly Algorithm (FA) for multimodal optimization applications. The proposed firefly algorithm is better than other optimization algorithm such as particle swarm optimization (PSO). Simulations and results indicate that the proposed firefly algorithm is superior to existing PSO algorithm.

Bishop et.al [16] discussed about relevance vector machine for increasing the classification accuracy. It is a probabilistic model whose functional form is equivalent to the SVM.

It achieves comparable recognition accuracy to the SVM, yet provides a full predictive distribution, and also requires substantially fewer kernel functions.

Deng et. Al [17] introduced the current problems of IoT in network security, and points out the necessity of intrusion detection. Several kinds of intrusion detection technologies are discussed, and its application on IoT architecture is analyzed. Li et. Al [18] proposes a novel algorithm using synergetic neural networks.

The algorithm first processes a meaningful gray watermark image, then embeds it as a watermark signal into the block Discrete Cosine Transform (DCT) component.

Li et. Al [19] introduced the history and current situation of intrusion detection system, expounds the classification of intrusion detection system and the framework of general intrusion detection, and discusses all kinds of intrusion detection technology in detail.

Sun et al. [20] presented a distributed detection mechanism that uses the dynamic time warping method to detect low-rate DDoS attacks. Based on the signature of the low-rate DDoS attack of a periodic short burst, they calculated the cumulative distance of the dynamic time warping between sampled flows and the template flows.

The cumulative distance of the dynamic time warping indicates the similarity degree between the two flows. However, as it is based on the periodicity of the attack flow, in theory, it may be vulnerable in real networks and under unknown signature patterns.

Luo et al. [21] proposed a mathematical model to evaluate the combined impact of attack pattern and network environment.

They analyzed the vulnerability of a system to sophisticated attack and the model of the minimum transmission rate of attack packets to tune the attack effect. Although the proposed model uncovers some novel properties of low rate DDoS attacks, more experiments using real datasets are needed to test their model.

Shevtekar et al. [22] proposed a lightweight data structure of packet arrival times at edge routers to detect low-rate DDoS attacks.

A flow meeting two conditions, namely, the burst length is greater than or equal to the RTT and the time period is equal to the fixed minimum RTO, is marked as malicious by their method.

However, they did not consider the network delay caused by network congestion, especially when a low rate DDoS attack is ongoing, and tested the performance only using simulation data.

III. LATENCY AND POWER AWARE RELIABLE INTRUSION DETECTION SYSTEM

Secondary cluster head is introduced to perform intrusion detection analysis before allowing traffic data into the primary server, so that network collusion can be avoided considerably.

Secondary cluster head selection is done based on trust values and resource availability such as energy and bandwidth.

Here Modified genetic algorithm is applied to select the secondary cluster head. In the modified genetic algorithm, modification is performed on the crossover by combining it with the mutation process.

Here the gene to undergone cross over is selected by using diversity based mutation scheme where the variance of genes is measured. The detailed explanation of the secondary cluster head selection procedure using modified genetic algorithm is given in the following sub sections.

3.1. Second Cluster Head Selection Using Modified Genetic Algorithm

A genetic algorithm is a search heuristic that is inspired by Charles Darwin's theory of natural evolution.

This algorithm reflects the process of natural selection where the fittest individuals are selected for reproduction in order to produce offspring of the next generation.

The process of natural selection starts with the selection of fittest individuals from a population.

They produce offspring which inherit the characteristics of the parents and will be added to the next generation.

If parents have better fitness, their offspring will be better than parents and have a better chance at surviving.

This process keeps on iterating and at the end, a generation with the fittest individuals will be found. Five phases are considered in a genetic algorithm.

"Initial population, Fitness function, Selection, Crossover, Mutation".

Initial Population: The process begins with a set of individuals which is called a Population. Each individual is a solution to the problem to solve.

An individual is characterized by a set of parameters (variables) known as Genes. Genes are joined into a string to form a Chromosome (solution).

In a genetic algorithm, the set of genes of an individual is represented using a string, in terms of an alphabet. Usually, binary values are used (string of 1s and 0s). We say that we encode the genes in a chromosome.

Fitness Function: The fitness function determines how fit an individual is (the ability of an individual to compete with other individuals).

It gives a fitness score to each individual. The probability that an individual will be selected for reproduction is based on its fitness score.

Selection: The idea of selection phase is to select the fittest individuals and let them pass their genes to the next generation. Two pairs of individuals (parents) are selected based on their fitness scores. Individuals with high fitness have more chance to be selected for reproduction.

Crossover: Crossover is the most significant phase in a genetic algorithm. For each pair of parents to be mated, a crossover point is chosen at random from within the genes.

Offspring are created by exchanging the genes of parents among themselves until the crossover point is reached. The new offspring are added to the population.

Mutation: In certain new offspring formed, some of their genes can be subjected to a mutation with a low random probability.

This implies that some of the bits in the bit string can be flipped. Mutation occurs to maintain diversity within the population and prevent premature convergence.

Termination: The algorithm terminates if the population has converged (does not produce offspring which are significantly different from the previous generation).

Then it is said that the genetic algorithm has provided a set of solutions to our problem.

The above procedure gives the overview of working procedure of genetic algorithm. I

n conventional genetic algorithm cross over points are selected randomly which might reduce the performance.

This is improved in this research method by introducing the modified genetic algorithm in which instead of selecting crossover points randomly, in this work diversity based mutation is integrated to select the cross over points optimally.

In the following sub section, detailed explanation about the diversity based mutation is provided.

In diversity based mutation scheme, more probability for mutation is given to a variable that has less population-wise diversity.

To implement, first the variance of values of each variable across the population members is computed and variables are sorted in ascending order of variance.

Thereafter, an exponential probability distribution ($p(i) = \lambda \exp(-\lambda i)$ for $i \in [0, n-1]$ is used.

To make the above a probability distribution, $\bar{\lambda}$ is used by finding the root of the following equation for a fixed n:

$$\lambda\exp(-n\lambda) - \exp(-\lambda) - \lambda + 1 = 0$$

Thereafter, for a random number $u \in [0, 1]$, the variable $(l + 1)$ that should be mutated is given:

$$l = \frac{1}{\lambda}\log\left(1 - u\left(1 - \exp\left(-n\bar{\lambda}\right)\right)\right)$$

For n = 15, $\bar{\lambda}$ = 0.168 is found.

Modified Genetic Algorithm is used for the selection of secondary cluster head based on Residual Energy, Bandwidth and memory.

Once the secondary cluster head was elected, data forwarding using minimum transmission power to the sink node is done.

Probability to become a server is more for a node with maximum RE, and maximum unused BW and maximum unused memory.

If any two of the parameters remain with maximum value and other one with minimum value, then probability of that node to become CH depends on the weights given for that parameter.

Algorithm for Cluster Head selection using Modified Genetic Algorithm

1. Produce an initial population of individuals with random chromosomes

2. Evaluate the fitness of all individuals and rank them

3. Select best individuals with maximum fitness function for reproduction

4. Remove some bad solutions from set

5. Recombine between best individuals

    Take any two individuals c1 and c2

    Apply diversity based mutation of c1

        Return gene g1 (node) with more variance

    Apply cross over between c1 and c2 on position g1

6. Evaluate the fitness of the modified individuals

7. Generate a new population

3.2. Dynamic Key Generation in Secondary Cluster Head

Our proposed method dynamic key generation for secured data sharing includes six phases which includes pre-phase, where each phase has its own process involved in authentication.

Pre-Phase: The node should register with a unique number and password with the secondary cluster head. During this phase node details are stored in the database of Authenticated node.

Phase 1: The nodes are connected to the secondary cluster head. Node communication and information are transmitted to the central processors that are connected to the servers. Here, services like AAA (Authentication, Authorization and Accounting) can be provided to the nodes based on Home Agent (HA) and subscriber's data stored in databases. The subscriber's requests are then delivered to a node through the Internet. During requesting phase the node has to provide his unique number/user id and password which was given in pre-phase.

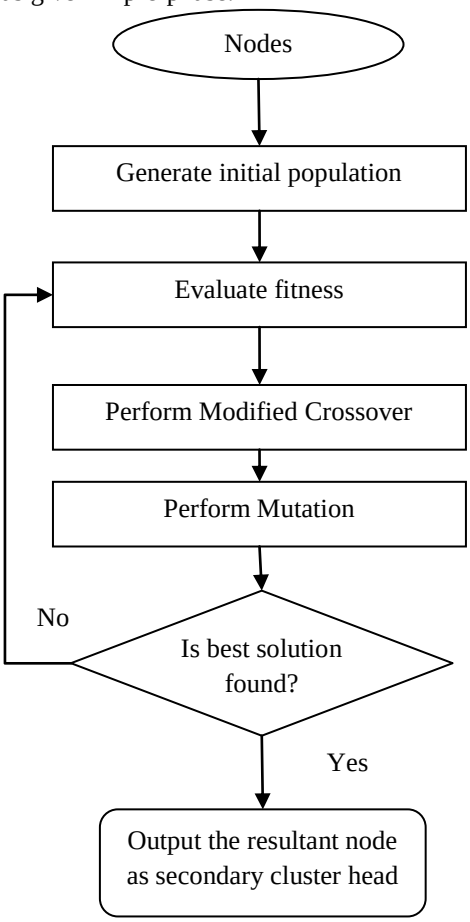

Figure 1: Flow Chart for Selecting Secondary Cluster Head

Phase 2: The secondary cluster head receives the user id and password provided by node and searches of the perfect match. If the id and password both the entities match then a confirmation notification message is sent along with dynamically generated key. The dynamic key is generated from the proposed encryption algorithm. If the user id and password did not match the message "accesses denied" is sent to the node.

Phase 3: In this phase of action, dynamic key is sent to the node on successful authentication during second phase. Dynamic key is a unique encrypted key which is generated and sent to node during each login session. It offers much higher security than static passwords, in expense of user friendliness and configuration issues.

Phase 4: Data transfer between node and server are taking place in an unreliable medium, so unique encryption and decryption method of key plays an important role in secure data transmission. The user receives the unique encrypted key which is generated by Key generator (using the proposed algorithm 1), on successful login in the previous phases. The decrypting application is given to the user only on successful registering and by accepting all the terms and conditions, regulations of the company; the decryption method is the reverse process of encryption. Nodes decrypt the key by using decryption application, there by node obtains the original key, this key is sent to the secondary cluster head to get access to the server.

Phase 5: In this phase the original key which is sent to the node after encryption and the key sent by node both are compared, if both the keys are matched then node is allowed to access the server. If the key does not match with that of the generated key for that node, then the access is denied. During this phase the control terminates if the key did not match, then the node has to go through all the phases once again to get access to the server. This happens only when the decrypted key is wrong or an unauthorized node tries to access the server.

3.3. Secured Data Encryption Using AES

Secure data communication is of a key concern in today's rapidly growing world. Various security mechanisms are developed in order to achieve the data security. Cryptography is one among them. It is the study of mathematical techniques that are related to the aspects of information security such as confidentiality, data integrity, authentication, and availability. The proposed architecture integrates the cryptographic algorithms, Advanced Encryption Standard algorithm (Symmetric) to improve the data security to a greater extent.

3.3.1. AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is a Federal Information Processing Standards (FIPS)-approved cryptographic algorithm that can be used to protect the electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) the data or information. Encryption process converts the data into an unintelligible form called ciphertext. Decryption converts back the ciphertext into its original form, called plaintext. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt the data in blocks of 128 bits. Encryption and decryption processes of AES are explained separately as follows:

Encryption process: The Encryption process of Advanced Encryption Standard algorithm for the proposed design is presented in Fig. 2. It consists of a number of transformations that will be explained later and these transformations are applied consecutively over the data

block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. Here user use 128-bit key so the number of rounds are 10. If the key length is 192-bit, then the number of rounds will be 12.

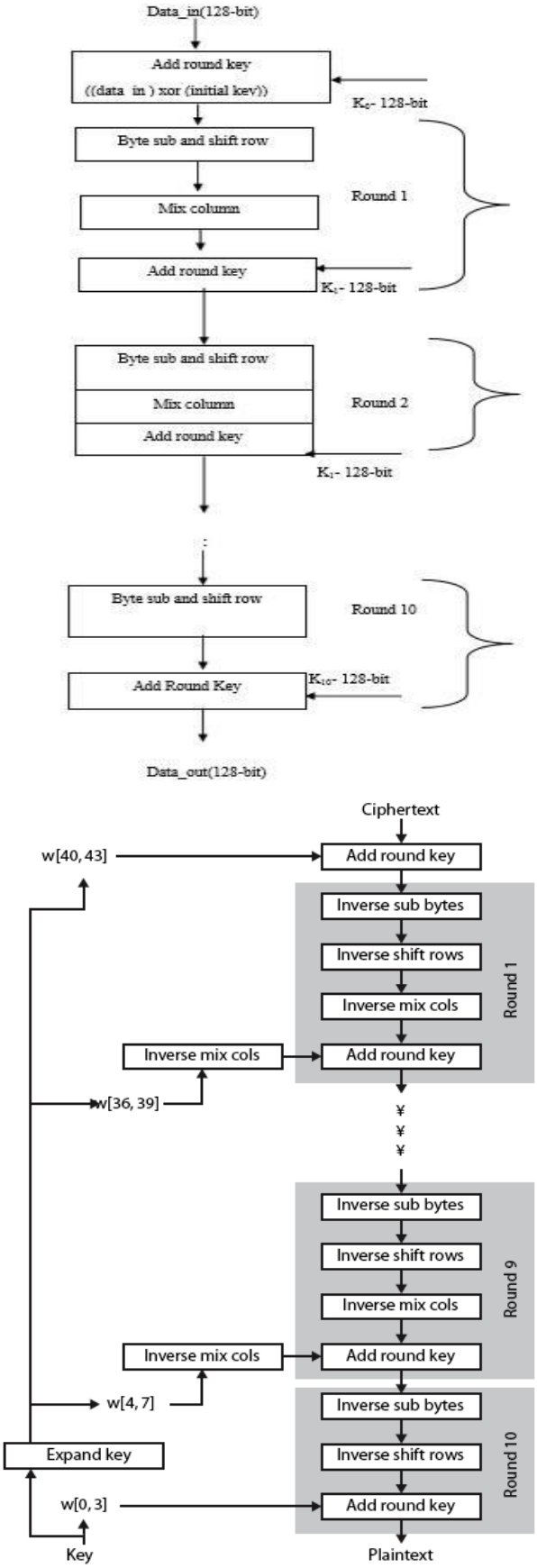

Figure 2: Encryption/Decryption of AES

Decryption process: The Decryption process of Advanced Encryption Standard algorithm is presented in Fig. 1. This is a process which is the direct inverse of the Encryption process. All the transformations applied in Encryption process are inversely applied to this process. Hence the last round values of both the data and key in encryption are the first round inputs for the Decryption process and this goes on in the decreasing order. The operations or transformations of AES algorithm for encryption and decryption can be explained as follows:

Sub Byte and Inverse Sub Byte Transformation: In the Sub Bytes step, each byte in the state matrix is replaced with a Sub Byte using an 8-bit data from the Rijndael S-Box. In the Inverse Sub Bytes step, each byte in the cipher matrix is replaced with corresponding Inverse Sub Byte. Sub Byte operation will provide the non-linearity in the cipher. The S-Box used is derived from the multiplicative inverse over Galois Field (2^8).

Shift Row and Inverse Shift Row Transformation: The Shift Rows transformation will perform the cyclic shifts of the bytes in each row by certain offset to the left. For AES, the first row remains unchanged. Each byte of the second row is shifted by one to the left. Similarly, the third and fourth rows are shifted by two and three respectively. Inverse Shift Row transformation does the same shift operation towards right.

Mix Column and Inverse Mix Column Transformation: This operation is basically a substitution but it makes use of arithmetic of GF (2^8). Each column is operated on individually. Here each byte of a column is mapped into a new value that will be a function of all four bytes in the column. Each element of the product matrix is the sum of products of elements of one row and one column. Here the individual additions and multiplications are performed in Galois Field (2^8). The inverse mix columns are performed in similar way but with different values in the matrix.

Add Round Key Transformation: In this operation, bitwise exclusive-or (XOR) operation is performed between outputs from Mix Column and Round Key. For AES-128, 128 bit XOR operations are performed.

IV. RESULTS AND DISCUSSION

In this section, the NS-2 simulator is used to evaluate the performance of the proposed Latency and Power aware Reliable Intrusion Detection System (LP-RIDS). This simulation model network consisting of 100 nodes placed randomly within a 100 × 100 meters area. The two types of nodes in the simulations are defined as: well-behaved nodes and malicious nodes. The malicious nodes can launch DOS attacks in the simulated scenarios. The BS has unlimited energy. The number of chosen CH is fixed to 10% for one interval. The proposed system performance is evaluated by comparing the proposed system LP-RIDSwith the previous systems namely Prioritization Based Delay Avoided Secured and Reliable Data Transmission Method

(PBDASRDT) and Attack Feature based Fast and Accurate Intrusion Detection System (AF-FAIDS) and existing system LEoNIDS [20].

The parameters used in this research for evaluating the trust system are given in the Table 1. The performance of LP-RIDS model was evaluated using the following metrics such as packet loss, packet delivery ratio, energy consumption, end-to-end delay, and mean packet latency.

Table 1: Simulation parameters

Simulation Parameters	Values
Channel	Wireless Channel
Mac	802.11
Antenna Type	Omni antenna
Routing Protocol	AODV
Initial Energy	100 joules
Traffic type	CBR
Agent	UDP
Simulation area	100X100 meters
Number of nodes	100

4.1. Packet Loss

The total number of data packets lost legitimately or through malicious action without any notification. Figure 3 shows the graphical representation of packet loss rate, it shows that the LP-RIDS method has lower packet loss rate when compared with the existing systems AF-FAIDS, LEoNIDS and PBDASRDT.

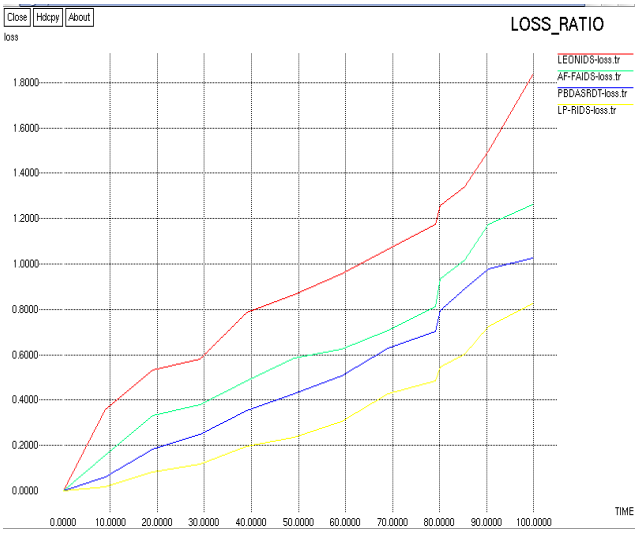

Figure 3: Comparison of packet loss in different trust model

The existing system doesn't focus on difference between the genuine nodes and the malicious as it considers every node with high traffic deviation as the malicious. The proposed algorithm identifies the individual malicious nodes based on bias and variance value thus the packet drop by the genuine nodes can be avoided. The experimental results shows that proposed LP-RIDS have lesser packet loss rate when compared existing AF-FAIDS, LEoNIDS and PBDASRDT.

4.2. Packet Delivery Ratio (PDR)

It is the ratio of the total number of data packets received to the total number of data packets transmitted. This illustrates the level of delivered data to the destination.

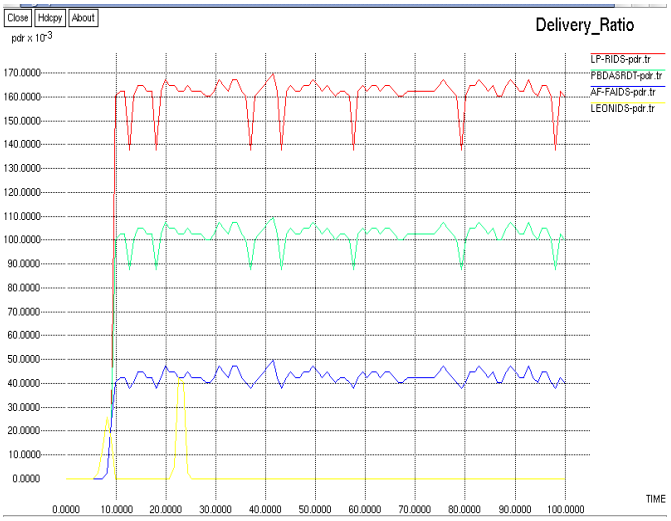

Figure 4: Comparison of packet delivery ratio for different trust system

Figure 4 shows the performance of the proposed LP-RIDS compared with AF-FAIDS, PBDASRDTand LEoNIDS with respect to the number of rounds and Packet Delivery Ratio (PDR). The number of packets which is effectively received at the destination without the loss of any packets or failure for the proposed LP-RIDS is high which shows higher PDR results.

4.3. Energy Consumption

The average energy consumed by each node during the given simulation time is expressed in Joules (J).

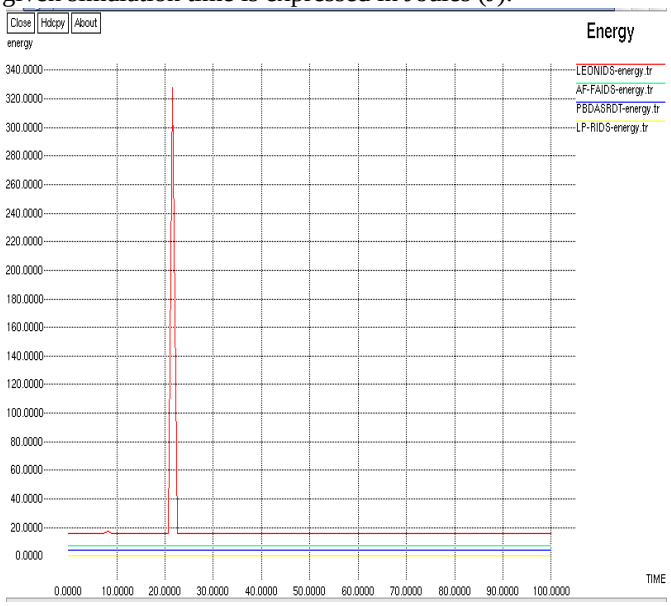

Figure 5: Comparison of energy consumption of different trust system

Figure 5 shows the graphical representation of energy consumption for different trust models of military applications. The LP-RIDS method has low energy consumption when compared with the existing system AF-FAIDS, LEoNIDS and PBDASRDT.

4.4. End-To-End Delay

It refers to the delay experienced by the data packet

during transmission from source to BS, including processing, queuing and propagation delay. The overall evaluation of these work is carried out on military applications. If hop to hop count distance value is high, it results high end to end Delay during path communication. Based on this hop to hop count distance data transmission is performed from source to destination in LP-RIDS system, so it results less end to end Delay. Since the proposed LP-RIDS system, high hop to hop count distance paths is not taken for data transmission.

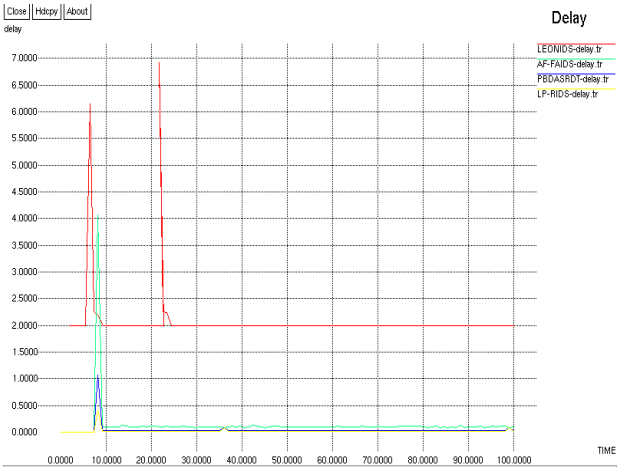

Figure 6: End-to-end delay comparisons for different trust system

The LP-RIDS method has low end-to-end delay when compared with the existing system AF-FAIDS, PBDASRDTand LEoNIDS. Proposed LP-RIDS system, high hop to hop count distance paths is not taken for data transmission and that path is considered as attack path.

4.5. Mean Packet Latency

The mean packet latency for those packets that reached the destination is lower for LP-RIDS since it is capable of selecting the shortest route with the lowest number of hops. And also mean packet latency is reduced in the proposed methodology due to reduced malicious attacks. The graphical representation of the mean packet latency is given in the following Figure 7.

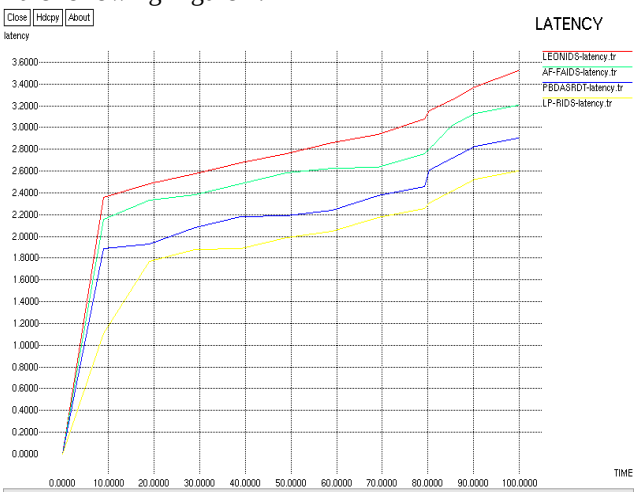

Figure 7: Mean packet latency

The LP-RIDS method has low packet latency when compared with the existing system AF-FAIDS,PBDASRDT, andLEoNIDS. Proposed LP-RIDSsystem, high hop to hop count distance paths is not taken for data transmission and that path is considered as attack path.

4.6. Routing Over Head

Routing overhead is defined as the computational overhead during routing process due presence of DoS attacks. Routing overhead of the proposed research method would be lesser.

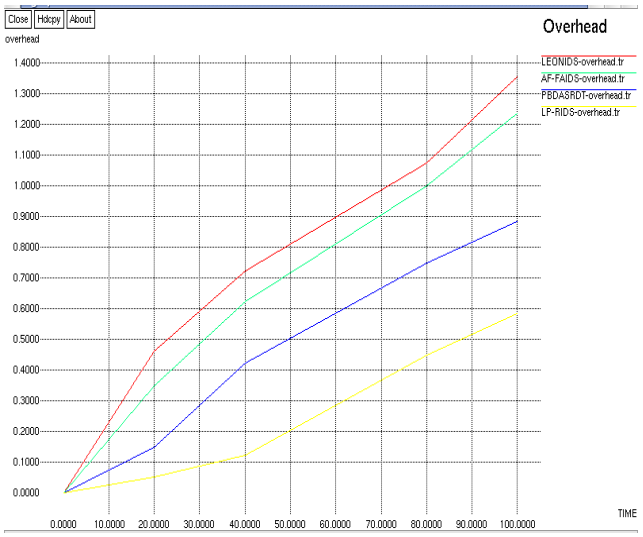

Figure 8: Routing Overhead comparison

The LP-RIDS method has low routing overhead when compared with the existing system AF-FAIDS,PBDASRDT, andLEoNIDS. Proposed LP-RIDSsystem, high hop to hop count distance paths is not taken for data transmission and that path is considered as attack path.

4.7. Detection Ratio

Detection ratio is the proportion of correctly predicting the IDS attacks present in the environment without fail. IDS attack detection ration should higher for the proposed research method for the ensured secured environment without IDS attacks presence.

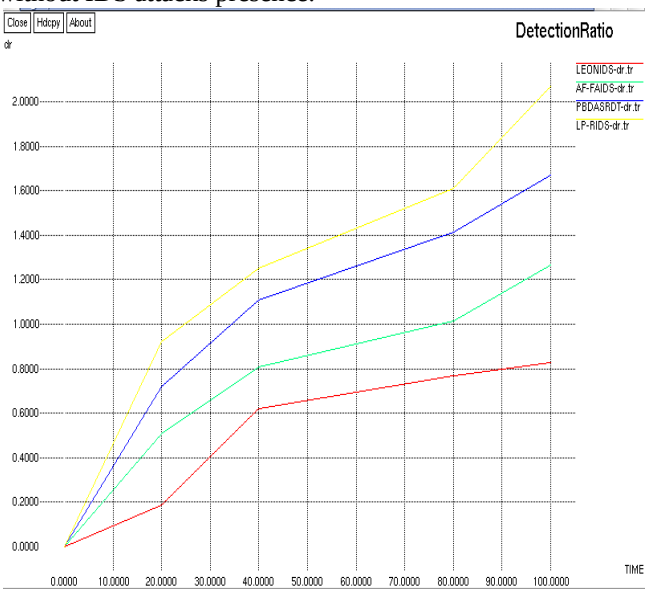

Figure 11: Detection Ratio comparison

The LP-RIDS method has higher detection ratio when

compared with the existing system AF-FAIDS, PBDASRDT, and LEoNIDS.

Proposed LP-RIDS system, high hop to hop count distance paths is not taken for data transmission and that path is considered as attack path

4.8. Numerical Analysis

In the following table 3, numerical values of the proposed simulation metrics obtained is given.

Table 3: Simulation parameter metric values

Time	Performance metrics											
	Packet Loss ratio				Delivery ratio				Energy			
	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS
10	0.38	0.18	0.1	0.07	5	40	100	160	18	2	1.5	1
20	0.56	0.36	0.2	0.1	0	46	107	167	18	2	1.5	1
30	0.6	0.4	0.28	0.13	0	43.5	104	164	18	2	1.5	1
40	0.8	0.5	0.36	0.2	0	45	106	166	18	2	1.5	1
50	0.88	0.6	0.44	0.25	0	47	107	167	18	2	1.5	1
60	0.98	0.63	0.52	0.3	0	45	104	163	18	2	1.5	1
70	1.19	0.74	0.64	0.42	0	43	102	162	18	2	1.5	1
80	1.2	0.95	0.8	0.55	0	38	100	160	18	2	1.5	1
90	1.5	1.18	0.98	0.72	0	45	105	165	18	2	1.5	1
100	1.83	1.25	1.02	0.82	0	40	100	160	18	2	1.5	1
Average	0.992	0.679	0.534	0.356	0.5	43.25	103.5	163.4	18	2	1.5	1
% improvement	64.11	47.5	33		32580	277	57.8		94.44	50	33	

Table 4: Simulation parameter metric values

Time	Performance metrics							
	Delay				Latency			
	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS
10	2	0.3	0.2	0.18	1.39	2.2	1.9	1.2
20	2	0.3	0.2	0.18	2.5	2.38	1.98	1.8
30	2	0.3	0.2	0.18	2.6	2.4	2.1	1.89
40	2	0.3	0.2	0.18	2.7	2.5	2.2	1.9
50	2	0.3	0.2	0.18	2.79	2.6	2.2	2
60	2	0.3	0.2	0.18	2.85	2.62	2.24	2.08
70	2	0.3	0.2	0.18	2.95	2.63	2.4	2.2
80	2	0.3	0.2	0.18	3.1	2.8	2.6	2.28
90	2	0.3	0.2	0.18	3.39	3.16	2.8	2.53
100	2	0.3	0.2	0.18	3.5	3.2	2.9	2.6
Average	2	0.3	0.2	0.18	2.777	2.649	2.332	2.048
% improvement	91	40	10		26.25	22.68	121	

Table 5: Routing overhead and detection ratio comparison

Time	Performance metrics							
	Routing Overhead				Detection ratio			
	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS	LEONIDS	AF-FAIDS	PBDASRDT	LP-RIDS
10	0.23	0.18	0.08	0.05	0.1	0.25	0.37	0.12
20	0.46	0.35	0.15	0.06	0.19	0.5	0.72	0.92
30	0.59	0.49	0.29	0.09	0.4	0.65	0.92	1.1
40	0.72	0.62	0.42	0.12	0.61	0.8	1.1	1.25
50	0.81	0.71	0.5	0.2	0.65	0.85	1.19	1.35
60	0.9	0.8	0.59	0.29	0.7	0.9	1.25	1.42
70	0.99	0.9	0.68	0.37	0.72	0.97	1.35	1.53
80	1.07	1	0.75	0.45	0.78	1.02	1.4	1.6
90	1.21	1.11	0.81	0.51	0.8	1.15	1.55	1.82
100	1.35	1.23	0.89	0.59	0.82	1.28	1.68	2.07
Average	0.833	0.739	0.516	0.273	.577	0.837	1.153	1.318
% improvement	67.22689	63.05819	47.09302		128.423	57.4671	14.3105	

V. CONCLUSION

In this work, intrusion detection is performed with the concern of metrics called latency and power consumption. The performance of the proposed research method is optimized by introducing the secondary cluster head selection process which is done by using modified genetic algorithm. This secondary cluster head is used to optimally balance the energy consumption and ensures the guaranteed verification of attack presence. The security of the proposed system is improvised by introducing the dynamic key based encryption technique which will be done in secondary cluster head by using which encryption will be done. In this work, AES techniques is utilized for the purpose of encryption. This methodology can improve the network performance considerably by detecting the attacks more accurately with reduced latency and delay. The overall evaluation of the research work is done in the NS2 simulation from which it can be verified that the proposed method assures the securing data sharing with the protection from the malicious nodes.

REFERENCES

1. McDermott, C. D., &Petrovski, A. (2017). Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks.
2. Ouffoué, G., Ortiz, A. M., Cavalli, A. R., Mallouli, W., Domingo-Ferrer, J., Sánchez, D., & Zaidi, F. (2016, June). Intrusion detection and attack tolerance for cloud environments: the CLARUS approach. In Distributed Computing Systems Workshops (ICDCSW), 2016 *IEEE 36th International Conference on* (pp. 61-66). IEEE.
3. Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2015). Taxonomy and survey of collaborative intrusion detection. *ACM Computing Surveys(CSUR)*, 47(4), 55.
4. Wang, L., & Jones, R. (2017). Big data analytics for network intrusion detection: A survey. *International Journal of Networks and Communications*, 7(1), 24-31.
5. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19-31.
6. Aljawarneh, S., Aldwairi, M., &Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152-160.
7. Fuller, J. D., Ramsey, B. W., Rice, M. J., &Pecarina, J. M. (2017). Misuse-based detection of Z-Wave network attacks. *Computers & Security*, *64*, 44-58.
8. Mitchell, R., & Chen, R. (2015). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 16-30.
9. Bul'ajoul, W., James, A., &Pannu, M. (2015). Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences*, *81*(6), 981-999
10. Singh, A., Sinha, P., & Bhattacharya, S. (2017). Detection and Localization of IDS Based Spoofing Attackers in Wireless Sensor Networks. *International Journal of Computer (IJC)*, *27*(1), 103-111.
11. Mrutyunjaya Panda and Manas Ranjan Patra, "A Comparative Study Of Data Mining Algorithms For Network Intrusion Detection", *First International Conference on Emerging Trends in Engineering and Technology*, pp 504-507, IEEE, 2008
12. Mohammadreza Ektefa, Sara Memar, Fatimah Sidi and Lilly Suriani Affendey, "Intrusion Detection Using Data Mining Techniques", pp 200-203, *IEEE*, 2010
13. Hu, Weiming, Wei Hu, and Steve Maybank. "Adaboost-based algorithm for network intrusion detection." Systems, Man, and Cybernetics, Part B: Cybernetics, *IEEE Transactions on* 38.2 (2008): 577-583.
14. Gao, Jun, et al. "Adaptive distributed intrusion detection using parametric model." Web Intelligence and Intelligent Agent Technologies, 2009. WI-IAT'09. *IEEE/WIC/ACM International Joint Conferences on*. Vol. 1. IET, 2009.
15. Yang, Xin-She. "Firefly algorithms for multimodal optimization." Stochastic algorithms: foundations and applications. *Springer Berlin Heidelberg*, 2009. 169-178.
16. Bishop, Christopher M., and Michael E. Tipping. "Variational relevance vector machines" Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence, *Morgan Kaufmann Publishers Inc.*, 2000.
17. Deng, Lianbing, Daming Li, Xiang Yao, David Cox, and Haoxiang Wang. "Mobile network intrusion detection for IoT system based on transfer learning algorithm." *Cluster Computing* (2018): 1-16.
18. Li, Daming, Lianbing Deng, Brij Bhooshan Gupta, Haoxiang Wang, and Chang Choi. "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications." *Information Sciences* (2018).
19. Li, Daming, Zhiming Cai, Lianbing Deng, Xiang Yao, and Harry Haoxiang Wang. "Information security model of block chain based on intrusion sensing in the IoT environment." *Cluster Computing* (2018): 1-18.
20. H. Sun, J. C. S. Lu, and D. K. Y. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proceedings of the 12th *IEEE International Conference on Network Protocols, ICNP* 2004, pp. 196–205, October 2004
21. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014
22. Shevtekar, K. Anantharam, and N. Ansari, "Low rate TCP denial-of-service attack detection at edge routers," *IEEE Communications Letters*, vol. 9, no. 4, pp. 363–365, 2005.