ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 4, April 2013

Detecting Anomalies Based On Entropy-Estimation

P.Karthik

Abstract— We know the sensor nodes perform monitoring and data collection tasks. It requires substantial protection and is exposing to node compromise which paves way to attackers when it is arranged in less protected environment. They interrupt the network communication by induction attacks in two ways such as dropping packets and modifying packets. Specifically, concession nodes drop or adjust the packets that they are thought to forward to destination. Nodes observe the forwarding behaviours of their neighbours incessantly to find out if their neighbours are mischievous. It is expanded by using the reputation based methods to permit nodes to finish whether a non neighbour node is trustable. The existing system utilizes Node labeling algorithm and Heuristic ranking algorithms to circumvent Packet dropping in which each packet is forwarded along compound redundant paths and avoid packet modifiers by sorting modified messages at en-route surrounded via a certain number of hops. But these countermeasures are not up to the level to moderate such attacks. This existing scheme decreases the false positive rate to slighter level but not to better coverage which in turn advances the accuracy of discovery of Packet Droppers and Modifiers. The proposed system intends at identifying low rate attacker because of the capacity of hiding attacker traffic comparable normal traffic. It has the capability to avoid the current anomaly-based recognition schemes. With various probability distributions, information metric can enumerate the disparities of network traffic. Thus intend two new information metrics such as the comprehensive entropy metric and the information distance metric to perceive low-rate attackers by measuring the divergence between genuine traffic and attack traffic. Therefore proposed information metrics can successfully notice low-rate packet droppers and modifiers attacks obviously and decrease the false positive rate.

.

Index Terms— Heuristic Ranking Algorithm, Packet Dropping, Anomaly-Based Recognition Scheme, Entropy Metric, Information Distance Metric, Wireless Sensor Networks, Packet-Forwarding Scheme, Intrusion Detection, IP Trace Back, Low-Rate Distributed Denial Of Service (DDoS) Attack.

I. INTRODUCTION

In a wireless sensor network sensor nodes check the environment, discover events of interest, produce data, and style, and collaborate in forwarding the data toward a sink which could be a gateway, base station, storage node, or querying user. Due to the simplicity of deployment, the low cost of sensor nodes and the competence of self-organization a sensor network is regularly deployed in an data unattended and hostile environment to carry out the monitoring and collection tasks. It lacks physical defence and is subject to node negotiation when it is deployed in such an environment. Later than compromising one or multiple sensor nodes, an adversary may initiate various attacks to interrupt the in-network communication. To deal with packet droppers are deployed, an extensively adopted countermeasure is multipath forwarding [1] wherein each packet is forwarded along multiple redundant paths and therefore packet dropping in some except not all of these paths can be tolerated. Most of existing countermeasures [2] aim to filter modified messages en-route to deal with packet modifiers within a certain number of hops. These countermeasures [2] can tolerate or moderate the packet dropping and modification attacks, but the impostors are still there and can persist attacking the network exclusive of being caught. To locate and identify packet droppers and modifiers, it has been planned that nodes constantly monitor the forwarding behaviours of their neighbours to resolve if their neighbours are mischievous.

The approach can be unmitigated by using the reputation based mechanisms to permit nodes to suppose whether a non neighbour node is trustable [3]. This methodology may be exposing to high-energy cost acquired by the immoral operating mode of wireless interface. In addition, the reputation mechanisms have to be implemented with cautions to circumvent or mitigate bad mouth attacks and formers. In wireless sensor network communications, an antagonist can achieve access to confidential information by monitoring transmissions between nodes. Encrypting sensor node communications partially solves eavesdropping exertions although needs a robust key exchange and distribution scheme. It must be simple for the network owner to carry out and sufficient for the limited sensor node hardware to execute. When an adversary compromises, it must also preserve confidentiality in the rest of the network, a few sensor nodes and depictions their secret keys. Preferably, these methods would as well permit revocation of known exposed keys and rekeying of sensor nodes. When it is deployed in less secured environment, it lacks physical protection and is subject to node compromise which overlays way to attackers. They interrupt the network communication by launching attacks in two ways such as dropping packets and modifying packets. Specifically, cooperation nodes drop or modify the packets that they are believed to forward to destination.

To avoid the problems in existing schemes, in this paper information-theory-based metrics have been projected to defeat the above restrictions. In information theory, information entropy [5] is a measure of the indecision connected with a random variable. Information distance (or divergence) appraise of the difference between different probability distributions. Shannon's entropy [5] and Kullback–Leibler's divergence methods have both been observed as effective schemes for distinguishing abnormal traffic based on IP address-distribution statistics or packet size-distribution statistics [4]. Early on detection and detection accuracy, for example low false positive rates, of DDoS attacks are the two most important criteria for the achievement of a protection system. In this paper, we productively recommend two new and effective anomaly-based detection metrics which not only recognize attacks previously, but also generate lower false positive rates when evaluated with the

Manuscript received March, 2013.
P.Karthik, *Computer science & Engineering, Anna University Chennai,, Coimbatore India, +919003457400*

traditional Shannon's entropy method and the Kullback-Leibler's divergence method.

The main involvement of the work is as follows:

1. We propose a straightforward thus far effective scheme, which can recognize misbehaving forwarders that drop or modify packets. That it can be deployed mutually with the false packet filtering schemes, and thus it cannot only identify intruders but also filter modified packets instantly after the alteration is detected.
2. It proposes the generalized entropy and information distance metrics outperform the traditional Shannon entropy and Kullback-Leibler's distance metrics for the low-rate DDoS attack detection in terms of early detection, lower false positive rates, and stabilities.
3. It plans an effective IP trace back scheme based on an information distance metric that can trace all attacks back to their own local area networks (LANs) in a little period of time.

The remainder of the paper is as follows: Section 2 describes the related works which is previously dealt by the researchers. The Section 3 deals with the proposed system. Section 4 explains the experimental results and discussion. The conclusion is described in Section 5.

2.RELATED WORK

Anthony et.al [6] explores denial-of-service vulnerabilities in WSNs. They started by groping terminology, the definition of denial-of-service, and why it is a potential problem for WSNs. Since vulnerabilities are along with the few parts of an attack under the control of the WSN exclusive, they reconsidered a variety of them along with possible defenses. A lot of solutions specified are not without cost; but they may be an essential price for enlarged robustness against DOS attacks. They looked to avoid DOS where that is possible, and detect, endure, and improve from the rest. Fan Ye et.al [7] We have developed SEF for false report detection. Authenticating event reports wants that nodes share confident security information; though, attackers can get such information by negotiation just a single node. To conquer this problem, SEF design separates a global key pool into multiple partitions and suspiciously assigns a certain number of keys from one partition to individual node. Min Cai et.al [8] have produced a scalable security overlay architecture, implied as NetShield for fast suppression of Internet worm eruptions and tracking of related DDoS flooding attacks. It presents DHT-based overlays for fast Internet security enforcement. The major powers of this approach recline in its high-speed, scalability, flexibility, and low complexity.

A new WormShield scheme is optional for automated worm signature detection and dissemination to prevent worm spreading. They also planned a cardinality-based counting method for tracking ATRs that forward most DDoS flooding attacks. Piyush Kumar Shukla et.al [9] referred Assessments of the existing Medium Access Control Protocols regarding handling augmented data traffic caused by spiteful Attacks. They aspire to expand an Attack Resilient approach for mounting the channel consumption for Medium Access Control Protocol. Ampah et.al [10] proposed IDS method takes to assist get rid of the following limits: imperfect scalability; effectiveness that is reducing false positive and false negative rates, efficiency and security. It also gets to counter DDoS attacks based on SYN-flood attacks or distributed attacks overall and also SYN flood attacks especially, if exercised as a back-up for existing IDSs. Seo Hyun Oh et.al [12] presented a malicious and malfunctioning node detection system using dual-weighted trust assessment in a hierarchical sensor network. Malicious nodes are effectively detected in the presence of natural faults and noise without sacrificing fault-free nodes. It, still, is urbanized for more realistic sensor networks, and can thus be practical to different structures exclusive of significant modifications.

3.PROPOSE WORK

A low-rate distributed denial of service (DDoS) attack has important capability of covering its traffic since it is greatly like normal traffic. A low-rate DDoS attack is an intelligent attack as the attacker can send attack packets to the victim at a sufficiently low rate to elude detection. The proposed system analyzes and highlights the advantages of generalized entropy [5] and information distance compared with Shannon entropy and Kullback Leibler distance. we proposes the generalized entropy and information distance metrics outperform the traditional Shannon entropy and Kullback–Leibler distance metrics for the low-rate DDoS attack detection in terms of early recognition, lower false positive rates, and stabilities. The information entropy is a calculation of the ambiguity associated with a random variable, structuring the origin for distance and divergence measurements among probability densities. We recommend an effective IP traceback method based on an information distance metric that can sketch all attacks support to their local area networks (LANs) in a short time. IP traceback is the facility to discover the source of an IP packet devoid of relying on the source IP field in the packet which is often spoofed. A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target thereby causing denial of service for users of the targeted system.

3.1 Classification of DDoS attack detection

DDoS attack detection metrics are mainly separated into two categories: the signature-based metric and anomaly-based metric. The signature-based metric depends on technology that deploys a predefined set of attack signatures such as patterns or strings as signatures to match incoming packets. The anomaly-based detection metric typically models the normal network traffic behaviour and deploys it to compare differences with incoming network behaviour. Anomaly-based detection has many limitations. First in anomaly-based detection systems attackers can train detection systems to gradually accept anomaly network behaviour as normal. Second, the false positive rate using the anomaly-based detection metric is usually higher than the one using the signature-based detection metric. It is difficult to set the proper thresholds which help to balance the false positive rate and the false negative rate. Third it is very difficult to extract the features of normal and anomalous network behaviours precisely. An anomaly-based detection metric uses a predefined specific threshold such as an abnormal deviation of some statistical characteristics from normal network traffic to identify abnormal traffic amongst all normal traffic.

Therefore the utilization and choice of statistical methods and tools is vitally important. It is generally accepted that the fractional Gaussian noise function can be used to simulate real network traffic in aggregation [6] and the Poisson distribution function can be used to simulate the DDoS attack traffic in aggregation. Therefore many information-theory-based metrics have been proposed to overcome the above limitations. In information theory information entropy is a measure of the uncertainty associated with a random variable. Information distance or divergence is a measure of the difference between different probability distributions. Shannon's entropy and Kullback–Leibler's divergence methods have both been regarded as effective methods for detecting abnormal traffic based on IP address-distribution statistics or packet size-distribution statistics. Early detection and detection accuracy such as a low false positive rate of DDoS attacks are the two most important criteria for the success of a defense system. The proposed system propose two new and effective anomaly-based detection metrics which not only

identify attacks but also produce lower false positive rates when compared with the traditional Shannon's entropy method and the Kullback–Leibler divergence method.

3.2 Generalized Entropy Metric

In information theory, the information entropy is a measure of the uncertainty associated with a random variable forming the basis for distance and divergence measurements between probability densities. If the information variable is more random it results in bigger entropy values. On the other hand if the information variable is more certain it results in smaller entropy values. The generalized information entropy as a generalization of Shannon entropy is used for quantifying either the diversity uncertainty or randomness of a system. Thus it is very important metric in statistics as an index of diversity. In order to observe and analyze the formulas of Shannon and generalized information entropy it is known that the high probability event can contribute more to the final entropy in generalized information entropy than in Shannon entropy while $\propto >$ 1. The low probability event can contribute more to the final entropy in generalized information entropy than in Shannon entropy while $\propto$ < 1. Therefore obtain different final entropy values by adjusting the $\propto$ value of generalized entropy in DDoS detection.

Information Distance Metric

In information distance metric there are three important properties of the information divergence such as additive, asymmetric and increasing function of $\propto$. The additive property is very useful because it implies that aggregated traffic can be seen as the sum of individual traffic which is then used in collaborative detection. The asymmetric property is an important property of information divergence as the direction of divergence used in detecting DDoS attacks can influence the effectiveness of the method. Thus it uses information divergence as a metric to overcome the asymmetric property by proposing the information distance such as Kullback–Leibler distance In information theory both information divergence and information distance are nonnegative values and the sum of the divergences or distances is always greater than themselves. In the meantime both the divergence and distance are increasing with order $\propto$. While $\propto >$, increase the divergence or distance between legitimate traffic and attack traffic to distinguish DDoS attacks easily and earlier by increasing the value of order and summing the divergences or distances in collaborative detection. Therefore in DDoS attack detection increase these properties of the information divergence and the information distance to enlarge the distance or gap between legitimate traffic and attack traffic to detect and raise alarms for DDoS attacks in the early hours accurately with a lower false positive rate.

3.3 Network model

A large number of sensor nodes are randomly deployed in a two dimensional area. Each sensor node generates sensory data periodically and all these nodes collaborate to forward packets containing the data toward a sink. The sink is located within the network which is aware of the network topology in which requiring nodes report their neighbouring nodes. The network sink cannot be compromised but the sensor nodes can be compromised to launch attack such as packet dropping and packet modification. In former the compromised node drops all or some of the packets that is supposed to forward. In latter the compromised node modifies all or some of the packets that is supposed to forward.

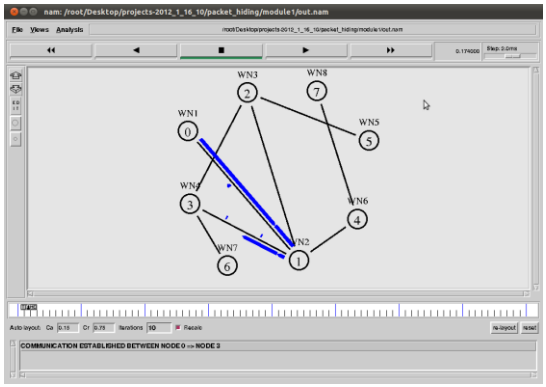

Fig : Packet sending

3.4 DAG Establishment to forward data

- Sensor nodes form a topology which is a directed acyclic graph (DAG). A routing tree is extracted from the DAG.
- In each round, data are transferred through the routing tree to the sink. The sink shares a unique key with each node.
- When a node wants to send out a packet, it attaches to the packet a sequence number, encrypts the packet only with the key shared with the sink and then forwards the packet to its parent on the routing tree.
- When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet and then forwards the packet to its parent.

3.5 Node categorization algorithm

When one round finishes based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad (i.e., packet droppers or modifiers) and nodes that are suspiciously bad (i.e., suspected to be packet droppers and modifiers).

- In attacker model, a misbehaving intermediate node may drop a packet it receives.
- On receiving a packet, the sink decrypts it and thus finds out the original sender and the packet sequence number.
- In each round, the sink tracks the sequence numbers of received packets for every node for every certain time interval.
- It calculates the packet dropping ratio for every node. Based on the dropping ratio and the knowledge of the topology, the sink identifies packet droppers.

The dropping ratio in this round is calculated as follows:

$$d_u = \frac{n_{u,flip} * N_s + n_{u,max} + 1 - n_{u,rcv}}{n_{u,flip} * N_s + n_{u,max} + 1}$$

Where U - Sensor node, $n_{u,max}$- Most recently seen sequence number, $n_{u,flip}$- Number of sequence number flips, $n_{u,rcv}$- Number of received packets and θ – Threshold.

- If a node's packets are not intentionally dropped by forwarding nodes, the dropping ratio of this node should be lower than θ.
- Else dropping ratio of this node is greater than θ, then it is due to droppers

3.6 Tree structure reshaping algorithm

The routing tree to forward data is dynamically changed from round to round so each sensor node have different parent node from round to round. It enables the sink to observe the behaviour of every sensor node in a large variety of routing topologies. After multiple rounds, the sink will collect information about node behaviours in different routing topologies. The parent node of node u is chosen based on those which are one hop closer to the sink and within node $u's$ communication range. Therefore, if node u choose node w as its parent in a round, node w will not select node u as its Parent and the routing loop will not occur. The selection is implicitly agreed between each node and the sink. Therefore, a misbehaving node cannot randomly select its parent in favour of attacks.

3.7 Heuristic ranking algorithms

For each of the round, node categorization algorithm is applied to identify sensor nodes that are bad for sure or suspiciously bad. After multiple rounds, sink further identifies bad nodes from those that are suspiciously bad from large number of suspiciously bad nodes; the sink runs heuristic ranking algorithms. The most likely bad nodes (S) are identified with the following properties

- **Coverage**: In any identified suspicious pair, at least one of the nodes in the pair must be in the set of most likely bad nodes
- **Minimality**: The size of S should be as small as possible in order to minimize the probability of misunderstanding innocent nodes.
- **Most-likeliness**: The node u must have higher probability to be bad based on n rounds of observation. Thus most-likeliness bad nodes are identified using several heuristics

A. Global ranking-based (GR) method:

The GR method is based on the heuristic that if a node is identified as suspiciously bad for more times, then it is bad node. With this method, each suspicious node u is associated with an accused account which keeps track of the times that the node has been identified as suspiciously bad nodes after n rounds of detection.

B. Stepwise ranking-based (SR) method:

It can be anticipated that the GR method will falsely accuse innocent nodes. So to reduce false accusation, SR method is used. With the SR method, the node with the highest accused account value is still identified as a most likely bad node.

- Once a bad node u is identified for any other node v that has been suspected together with node u, the value of node v's accused account is reduced by the times that u and v have been suspected together.
- This adjustment is motivated by the possibility that v has been framed by node u.
- After the adjustment, the node that has the highest value of accused account among the rest nodes is identified as the next mostly like bad node which is followed by the adjustment of the accused account values for the nodes that have been suspected together with the node.
- This process continues until all suspicious pairs have been removed.

C. Hybrid ranking-based (HR) method

The GR method can detect most bad nodes with some false accusations while the SR method has fewer false accusations but may not detect as many bad nodes as the GR method.

But according to HR, the node with the highest accused account value is still first chosen as most likely bad node. After a most likely bad node has been chosen, the one with the highest accused account value among the rest is chosen only if the node has not always been accused together with the bad nodes that have been identified already.

3.8 Generalized Entropy Metric

The information entropy ***H (x)*** is a measure of the uncertainty associated with a random variable, forming the basis for distance and divergence measurements between probability densities. The generalized information entropy as a generalization of Shannon entropy is for quantifying either the diversity uncertainty or randomness of a system.

$$H_1(x) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

3.8.1 Information Distance Metric

Consider two discrete complete probability distributions p and q. The information divergence is a measure of the divergence between p and q is shown below. This aggregated traffic can be seen as the sum of individual traffic and therefore form the basis of the collaborative detection or multipoint detection

$$D_\alpha(P||Q) = \frac{1}{\alpha - 1}\log_2\left(\sum_{i=1}^{n} p_i^\alpha q_i^\alpha\right)$$

Algorithm to mitigate packet droppers and modifiers:

1. Set the sampling frequency, sampling period and the collaborative detection threshold.
2. Sample the network traffic comes from the upstream routers and LAN in parallel.
3. Calculate in parallel the numbers of packet which have various recognizable characteristics (e.g., the source IP address or the packet's size, etc.) in each sampling time interval within threshold.
4. Calculate the probability distributions of the network traffic come from LAN and router in parallel.
5. Calculate their distances on router using the formula of Sum the distances.

$D_\alpha(P,Q) = D_\alpha(P||Q) + D_\alpha(Q||P)$

7. If the summed distance is more than the collaborative detection threshold, then the system detects the attackers and begins to raise an alarm and discards the attack packets; otherwise the routers forward the packets to the downstream routers.
8. Return to step 2

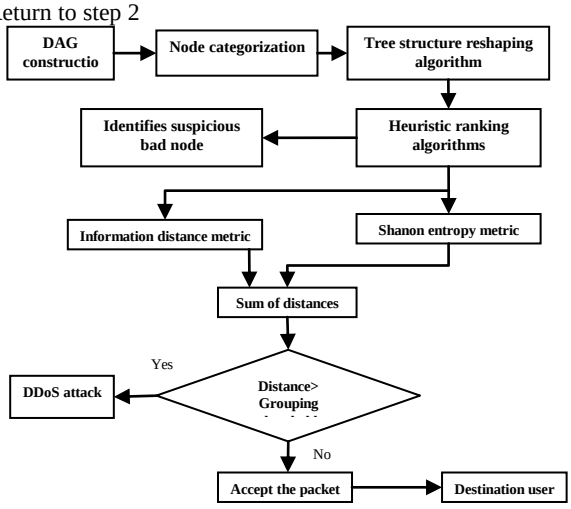

Fig 1: Architecture diagram

The architecture exposes an effective scheme to grasp both packet droppers and modifiers with condensed false positive rate. In this proposal a routing tree origin at the sink is first recognized. When sensor data are spread along the tree structure toward the sink every packet sender or forwarder appends a small number of more bits which is called packet marks to the packet. The design of the small packet marks is intentionally designed such that the sink can attain very useful information from the marks. Based on the packet marks

the sink can understand the dropping ratio associated with every sensor node and then runs node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/ modifiers. In this way most of the bad nodes can be increasingly recognized with small false positive. Thus the proposed system aimed at reducing false positive rate to larger point. The information metric can detail the differences of network traffic with different probability allocations by proposing using two new information metrics such as the generalized entropy metric and the information distance metric to perceive low-rate DDoS attacks by measuring the difference between genuine traffic and attack traffic with threshold. If distance is greater than the combination threshold it is assured as low rate DDoS attack packet else recognize it and forward to the destination.

1. RESULTS AND DISCUSSION

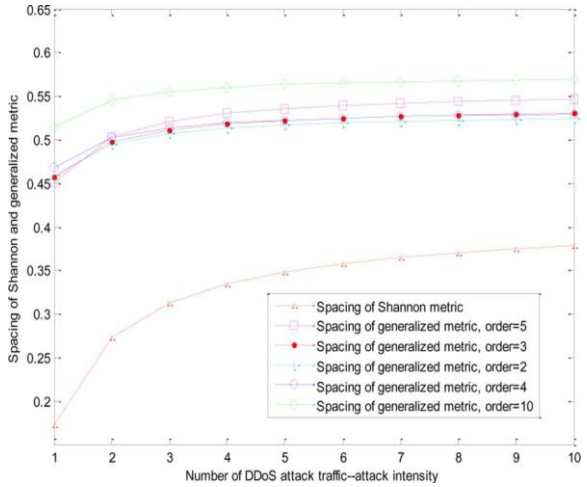

Fig 2: Variations of spacing of Shannon and generalized metrics

This Fig 2: indicates that the spacing of Shannon and generalized metrics are increasing along with the increasing of number of DDoS attack traffic. There are rapid increases of spacing at the beginning period whatever the Shannon or generalized metric, because the attacks still are low-rate attacks during this period.

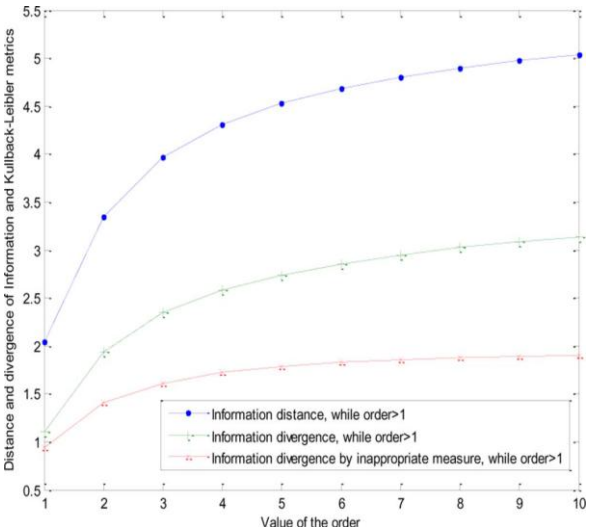

Fig 3: Variations of distance of the information and Kullback–Leiblermetrics

To facilitate test deviations of distance and divergence of the Kullback–Leibler metric and information metric with the order α, the normal network traffic and the low-rate attack traffic must have the same number of source IP addresses in a sampling period and the graph shown as Fig 3. As a result, we sample the above low-rate DDoS attack traffic over again to form a new low-rate attack which will have the same number of source IP addresses with the normal traffic, and have the same probability distribution of source IP addresses with the original attack traffic.

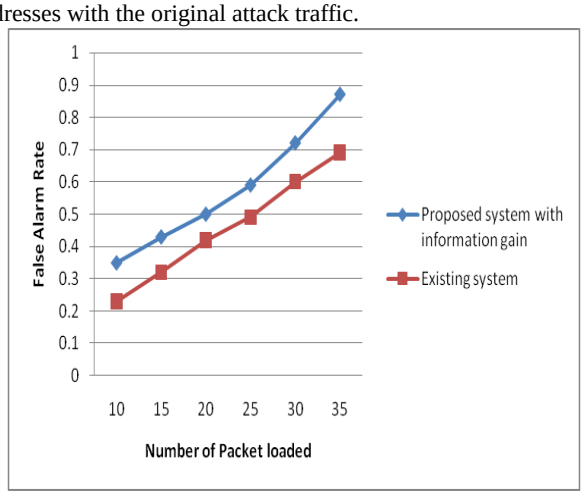

Fig 4: False Alarm Rate Evaluation

This graph shows the False Alarm rate of existing and proposed system based on two parameters of False Alarm Rate and the number of packets. From the graph we can see that, when the number of packets is improved the False Alarm also improved in proposed system but when the number of packets is improved the False Alarm is reduced somewhat in existing system than the proposed system. From this graph we can say that the False Alarm of proposed system is increased which will be the best one. In this graph we have chosen two parameters called packets and False Alarm which is help to analyze the existing system and proposed systems. The False Alarm rate will be the Y axis and the packets parameter will be the X axis. The blue line represents the existing system and the red line represents the proposed system. From this graph we see the False Alarm of the proposed system is higher than the existing system. Through this we can conclude that the proposed system has the effective False Alarm Rate.

2. CONCLUSION AND FUTURE WORK

The method identifies misbehaving forwarders that drop or modify packets. Every packet is encrypted and padded in order to hide the source of the packet. The packet smudge, a small number of additional bits is included in each packet such that the sink can recuperate the source of the packet and then understand the dropping ratio connected with every sensor node. The routing tree structure dynamically modifies in each round thus behaviours of sensor nodes can be experiential in a large variety of scenarios. At last, the majority of bad nodes can be known by our heuristic ranking algorithms with small false positive. While the proposed metrics can increase the information distance among attack traffic and legitimate traffic they can efficiently detect low-rate DDoS attacks early and decrease the false positive rate obviously. The success and competence of the proposed method are estimated in the ns-2 simulator to recognize mischievous forwarders that drop or modify packets. Thus far base paper is implemented with false positive rate. In the forthcoming duration false positive rate is removed entirely. Thus our proposed information metrics can considerably advance the performance of low-rate DDoS attacks exposure.

REFERENCES

[1] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. IEEE First Int’l Workshop Sensor Network Protocols and Applications, 2003.

[2] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, 2004.
[3] W. Li, A. Joshi, and T. Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach," Proc. 11th Int'l Conf. Mobile Data Management (MDM '10), 2010.
[4] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Netw., vol. 51, no. 12, pp. 3448–3470, 2007.
[5] C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol. 27, pp. 379–423 and 623–656, 1948.
[6] Anthony D. Wood and John A. Stankovic,"A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Department of Computer Science, University of Virginia
[7] Fan Ye, Haiyun Luo, Songwu Lu,"Statistical En-Route Filtering of Injected False Data in Sensor Networks", IEEE Journal On Selected Areas In Communications, VOL. 23, NO. 4, APRIL 2005
[8] Min Cai, Kai Hwang, Yu-Kwong Kwok, Shanshan Song, and Yu Chen,"Fast Containment of Internet Worms and Tracking of DDoS Attacks with Distributed-Hashing Overlays", Nov/Dec. 2005.
[9] Piyush Kumar Shukla,S. Silakari, S.S. Bhadouria, "Designing And Analysis Issues For An Attack Resilient and Adaptive Medium Access Control Protocol for Computer Networks: An Exclusive Survey", May 30, 2009
[10] Ampah, N. K., Akujuobi, C. M. and Annamalai, A.,"An Intrusion Detection Technique Based on Discrete Binary Communication Channels", (2011)
[11] Prateek Suraksha Bhushan, Abhishek Pandey, and R.C. Tripathi,"A Scheme for Prevention of Flooding Attack in Wireless Sensor Network", Vol. 1, No. 2, June 2011
[12] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi,"A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks", Wireless Sensor Network, 2012, 4, 84-90
[13] Mieso K. Denko,"Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", volume 3 - number 4

P.KARTHIK RECEIVED HIS B.TECH INFORMATION TECHNOLOGY DEGREE FROM ANNA UNIVERSITY, COIMBATORE IN 2011 AND PURSUING M.E COMPUTER SCIENCE AND ENGINEERING DEGREE FROM ANNA UNIVERSITY,CHENNAI, INDIA, HIS PG PROJECT INTERESTS ARE IN THE AREAS OF WIRELESS SENSOR NETWORKS IN SECURING TRANSMISSION .