IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 47-53

Giant Sheltered Interloping Endurance System in Divergent Wireless Sensor Network Network Security Algorithm

R.Sivaranjani, Sharmila Banu
Research scholar providence College for women Affliated to Bharathiar University
Assistant Professor of Providence college for women

Abstract: *Real Time interloping endurance system in divergent wireless sensor networks is proposed in this study, to minimize the redundancy and maximize the tolerance life time through increasing mean time to repair on nodes and analyzing Mean time Between Failures. Multipath routing helps in successful completion of the task, but identifying the malicious nodes between divergent networks and surpassing them is often energy consuming and time-delayed. In order to overcome this, a real time system was formulated by identifying the Mean time to repair and the mean time between failures in multipath routing. When there are more than two nodes in the divergent network are identified as malicious, the Mean Time to Repair is applied on the specific network so as to rely on the particular network's tolerance and once the decrease in mean time to repair is achieved the routing resumes with a delay time of acceptable mean time between failures. As this type of tolerance monitoring system helps network operators and server managed service providers to maximize security and an undisruptive process completion without any drop-offs, which can gain advantage in less energy consumption and reduce network compromises. Giant sheltered Interloping endurance system in divergent wireless sensor network*

Keywords: *Interloping detection, interloping endurance, Redundancy minimization, secure transmission*

I. Introduction

All nodes in the same network and or on a different network collectively maintain the network connectivity. This type of network is employed in situations like, where there is a need for a temporary or an uninterrupted network connection. It is evident that maintaining an uninterrupted connection often consumes energy and time. Recent development in research on QOS and energy management has proposed lot of theories and some are proven to be effective in All nodes in the same network and or on a different network collectively maintain the network connectivity. This type of network is employed in situations like, where there maximizing the performance of QOS and energy management.

In terms of QOS, i.e reliability, Timeliness and security, multipath routing is found to be an effective method during fault endurance and intrusion tolerance. Multipath routing between heterogeneous networks are the most challenging aspects with regards to QOS and Energy Management as the node take a vital role in collecting and routing of intellect data [7]. For redundancy management and intrusion detection, more number of literatures and thesis are available. While identifying the malicious nodes and multipath routing may be achieved with other techniques, in terms of QOS, identifying the more than two nodes in multipath routing in quiet challenging.

In this paper we propose an intrusion tolerance system where malicious nodes are identified with in the network and the tolerance level of the identified network is evaluated to carry out the routing further using a system that allows an increase of mean time to repair within the network and measure the tolerance level of the system without changing the policies of the heterogeneous networks. As this type of tolerance monitoring system helps network operators and server managed service providers to maximize security and an undisruptive process completion without any drop-offs, which can gain advantage in less energy consumption and reduce network compromises.

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as traceroute. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packets, it is often harder to detect because some traffic still flows across the network.

The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast

that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

Among various types of denial of service attacks, "dropping attack" is probably the most difficult one to handle. This paper explores the negative impacts of packet dropping attacks and a method to detect such attacks. First, three dropping patterns are classified and investigated. We demonstrate that attackers can choose different dropping patterns to degrade TCP service to different levels, and selectively dropping a very small number of packets can result in a severe damage to TCP performance. Second, we show that a hacker can utilize a DDoS attack tool to control a "uncompromised" router to emulate dropping attacks. This proves that dropping attacks are indeed practically very possible to happen in today's Internet environment. Third, we present a statistic analysis module for the detection of TCP packet dropping attacks. Three measures, session delay, the position and the number of packet reordering, have been implemented in the statistic module. This paper has evaluated and compared their detection performance.

Generally, packet dropping attacks can impact a network service on the following several aspects: Delay: e.g., dropping the retransmissions of packets in a FTP connection will drastically increase the total file transfer time; Response time: e.g., if the DNS query packets are dropped, a user may feel waiting for a long time to get a web page; Quality: e.g., dropping some packets of MPEG video stream or IP telephoning data flow can degrade the quality of the service; Bandwidth: because dropping packets usually introduces packet retransmissions, which waste network bandwidth. In this paper, we study how packet dropping attacks affect FTP file transfer. Since file transfer services have comparatively low requirements on response time and quality, we focus on the dropping attacks' negative impacts on session delay.

We distinguish two types of dropping attacks, persistent and intermittent dropping attacks. The former performs attacks on every FTP connection, while the later only attacks a portion of the connections. For example, an intermittent attacker can attack 20% of all the connections (i.e., one in every five). An attacked connection is called a victim connection and packets dropped by attackers are called victim packets.

WSNs are mostly unguarded and the wireless medium is inherently broadcast in nature. This makes WSNs vulnerable to all kinds of denial-of-service (DoS) attacks. Without proper security measures, an adversary can launch various kinds of attacks in hostile environments. These attacks can disrupt the normal working of WSNs and can even defeat the purpose of their deployment. An adversary can launch some attacks without even cracking keys used for cryptography-based solutions. DoS attacks (like packet dropping, false route request, or flooding) can deplete the network of energy without much effort on the part of an adversary. Therefore, intrusion detection mechanisms to detect DoS attacks are needed. To be practical for implementing on WSNs, solutions for detecting intrusions should be lightweight

II. Related Works

In earlier, several protocols have been proposed to detect intrusion in WSNs. [1], [2] provide excellent surveys of the subject. In [3], a decentralized rule based intrusion detection system is proposed by which observer nodes are having authority to monitoring neigh boring nodes. The monitor nodes apply predefined rules to collect messages and it gives alarms if the number of failures goes above a threshold value.

We investigates the usefulness of multi-path routing [4] to achieve lifetime improvements by load balancing and exploiting cross-layer information in wireless sensor networks. Presentation increase in the order of 10-15 % could be achieved by altering path update rules of existing on-demand routing method. Complications meet with corresponding traffic along interfering paths have been identified as a direct consequence of special MAC protocol properties.

In a WSN, there are two ways for the detection of an intruder: single-sensing detection and multiple-sensing detection. In single sensor detection, intruder can be successfully detected but multiple-sensing detection the intruder can only be detected by multiple sensors. In some applications; the sensed information provided by a single sensor might not be adequate for recognizing the intruder, because single sensors can only sense a percentage of the intruder. The detection can be examined according to the capability of sensors over the transmission range and sensing range.

In a heterogeneous WSN specific sensors have a enormous capacity to achieve a longer transmission range and large sensing range. Recent studies [8], [9] demonstrated that using heterogeneous nodes can enhance performance and prolong the system lifetime. Finally, nodes with greater resources serve as CHs performing computationally intensive tasks while low-cost with less capacity SNs are essentially used for sensing the environment. Thus, the heterogeneous WSN increases the intrusion exposure possibility for a available intrusion detection system. It is commonly believed in the research community that clustering [10], is an effective

solution for achieving scalability, energy conservation, and reliability. Therefore the cluster based heterogeneous WSN can improves the performance of the network.

We describe an Intrusion-tolerant routing protocol for wireless Sensor Networks (INSENS) [5]. INSENS make onward tables at each node to make easy communication between sensor nodes and a base station. It ease working out, storage, bandwidth and communication requirements at the sensor nodes in the cost of better computation, storage, bandwidth and communication requirements. INSENS is not available on recognize the intrusions, other than slightly tolerates intrusions by sidestep the malicious nodes. A very important possession of INSENS is that while a malicious node may be able to cooperation a small number of nodes in its region, it cannot reason extensive damage in the network.

The authors use watchdogs that identify misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. When a node forwards a packet, the nodeís watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next nodeís broadcast transmissions. If the next node does not broadcast the packet, it is misbehaving and the watchdog detects it. Every time a node fails to forward a packet, the watchdog increments the failure-tally. If the tally exceeds a certain threshold, it is determined that the node is misbehaving; this node is then avoided with the help of the pathrater. The pathrater combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. The overhead of passive continuous passive listening is formidable for WSNs.

Buchegger [4] proposed a mechanism that detects misbehaving nodes by means of observations or reports about several types of attacks. This allows nodes to find routes around misbehaving nodes and to isolate them from the network. Nodes have a monitor for observations, reputation records for first-hand observations and trusted second-hand reports, trust records to control trust given to received warnings, and a path manager to adapt their behavior according to reputation of other nodes. This approach involves continuous monitoring similar to Martiís approach and collecting information about intrusion detections at other places in the network. The overhead is prohibitive for WSNs.

Michiardi. [8] Proposed a collaborative reputation mechanism that has a watchdog component. However, it is complemented by a reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task specific behavior). They are weighted for a combined reputation value used to make decisions about cooperation with or gradual isolation of a node. This approach involves continuous monitoring and collecting information about intrusion detections at other places in the network for specific functions. The overhead is too high for WSNs.

Marti [6] discussed two techniques that detect compromised nodes that agree to forward packets but fail to do so. The authors use watchdogs that identify misbehaving nodes and a path rater that helps routing protocols avoid these nodes. When a node forwards a packet, the node ís watchdog verifies that the next node in the path also forwards the packet.

III. Proposed Methodology

I. Malicious Nodes And Detection

WSN encompasses different capability types of sensors are Cluster Heads (CHs) and Sensor Nodes (SNs). The identification of sensor nodes that are malicious is ruled out using various network policies among the heterogeneous networks and it is assumed that nodes that violates the policies of a network and are named as fault is considered.

To find cooperated nodes, every node runs a simple host IDS to assess its neighbors. Our host IDS is light-weight to preserve the energy. It is a common manner and does not rely on the feedback mechanism tied in with a specific routing protocol For example, MDMP for WSNS or AODV for MANETs. It is based on local monitoring. That is, each node monitors its neighbor nodes only and those nodes uses a set of anomaly detection rules such as a high discrepancy in the sensor reading or recommendation even though the packet is not forwarded as requested, as well as interval, retransmission, repetition, and delay rules as in. If the count exceeds a system-defined threshold, a neighbor node that is being monitored is considered compromised. The failure of monitoring due to environment noise or channel error is modeled by a “host” false positive probability (Hpfp) and a “host” false negative probability (Hpfn) which are assumed known at deployment time [6].

II. QOS Policies

A. Mean Time between Node Failures

In every network, the routing protocol comprises of QOS metrics such as bandwidth limitation, removal of redundancy, energy and time trade-off, buffer size limitation, to support multiple traffics, and power states like ready, idle, and suspend. In heterogeneous multipath routing, the mean time standards are based on

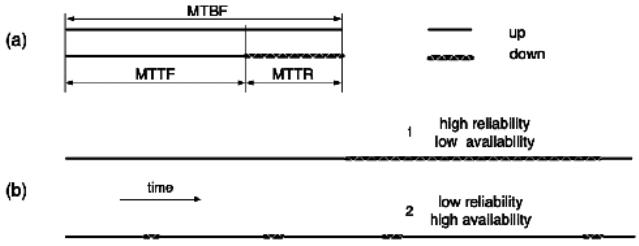
the network policies between other networks. Generally (Mean Time to Failure) MTTF is defined as, the number of instances the system can answer or process effectively. When there is no process takes place, i.e. no answers or functions, then it is said to be failed. In general the failure has been occurred before the deadline. The causes to the failure may involve many reasons such as energy exhaustion, a packet dropping, or insufficient transmission speed, time delay etc.

The time difference between two consecutive failures is termed as Mean Time between Failures (MTBF), usually, the network QOS or network policies are pre-built with a Mean Time To Repair (MTTR) allowing nodes to get reset their identity base on the intrusion level or intrusion type. With the Time to Repair, the malicious nodes are rectified or quarantined as malicious during the routing process.

MTBF = TIME DIFFERENCE BETWEEN SUCCSSIVE FAILURES

OR

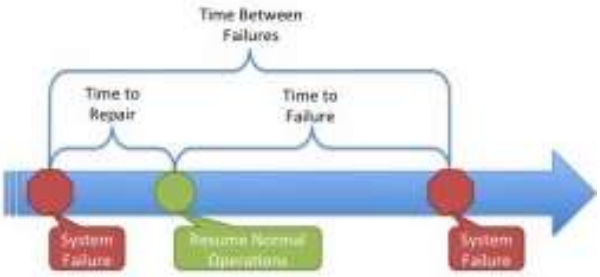
$$MTBF = \frac{\text{FIRST MTTF} - \text{SECOND MTTF}}{\text{TIME}}$$



B. Mean Time to Repair

The Time required for a node to restore to its original state is termed as Mean Time To Repair (MTTR). Generally the node repair is based on the network QOS policy, like bandwidth, signal power, noise level, processing signal strength, computational energy levels etc. the wireless sensor reliability is also achieved through reading of data sent.

In our proposed model, whenever there is an instance of malicious node of more than one, the corresponding node which encounters the second malicious node in multipath routing inside a cluster, automatically increases the mean time of the first node to that particular network, and gathers other credentials to established the intrusion or clear state,. The network in return assures the reliability of the node with various parameters such as identity, operational faults, redundancy level, etc., and allows the time to repair, once the time to repair is finished a security credentials are compared and assigned a repaired nodes or quarantined nodes. This process ideally finds out the frequency of intrusions, intrusion types, and location which strengthens the network reliability. If the node is said to be compromised, then the routing process halts and the data packets are dropped, allowing a secured routing between heterogeneous networks. Although this may consume some energy cost, in terms of intrusion tolerance, the redundancy rate between the networks can be lowered and also compromised nodes can be distinguished between physical levels or intrusion levels.



Difference between Failures

III. Implementation Results

A. Tolerance between Heterogeneous Networks

We proposed a distributed, randomized clustering algorithm to organize the sensors in a wireless sensor network into clusters. This clustering enables to identify the outliers, anomaly, and the outcome from the sensor

node. This approach on distributed clustering identifies the long-lived sensor nodes within the networks. The long-lived nodes can be classified based on the intruder type, such as external intruder or an internal intruder. Once those nodes that are identified as compromised, a additional mean time is applied on every node to assert that truly the nodes are compromised.

Multi-path routing protocols can enhance the degree of fault tolerance by having redundant information routed to the destination in multipath. This tolerance can helps to reduce the probability of the communication is disrupted and data is lost in case of link failures the exchange between the additional overheads and the reliability. The clusters head share a pair-wise key between the nodes in the multipath within the cluster, thus securing the network lifetime and reducing the packet drops.

B. Query Processing Redundancy Rate

The query processing redundancy rate can be measured through determining the cluster threshold and its response time. This response time is same such that the lag-time we manually assign to nodes in case of fault. The mean time (lag time) to repair is observed within the cluster eliminating the outliers. Also by comparing the incoming query rate and the outgoing query rate in multipath, the redundancy rate can be arrived using the formula,

$$C = \frac{\mu}{\lambda + \mu} = \frac{MTBF}{MTBF+MTTR}$$

Where, $\mu = \frac{1}{\tau}$

τ is the average time required to repair,

λ is the average time loss with n failures with t time

C. Detection Accuracy

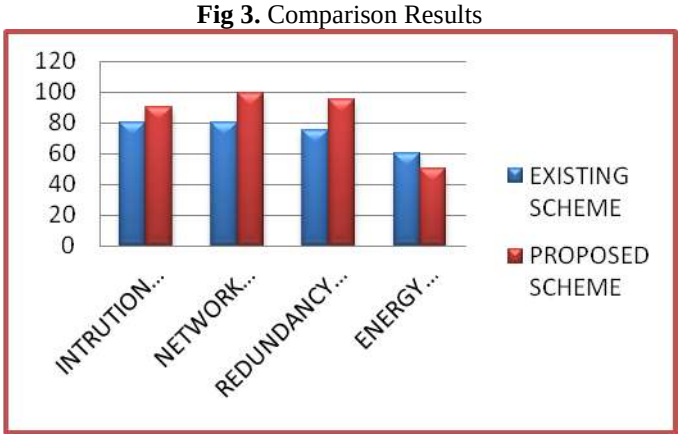
A New proposed approach improves the malicious detection rate and tolerates those nodes with minimum time and energy consumption, even though the redundancy minimization also efficiently implemented.

Table 1

Method	Intrusion Detection (%)	Network Tolerance (%)	Redund -ancy Rate (%)	Energy Consum- Tion(%)
Existing scheme	80	80	75	60
Proposed Scheme	90	98	95	50

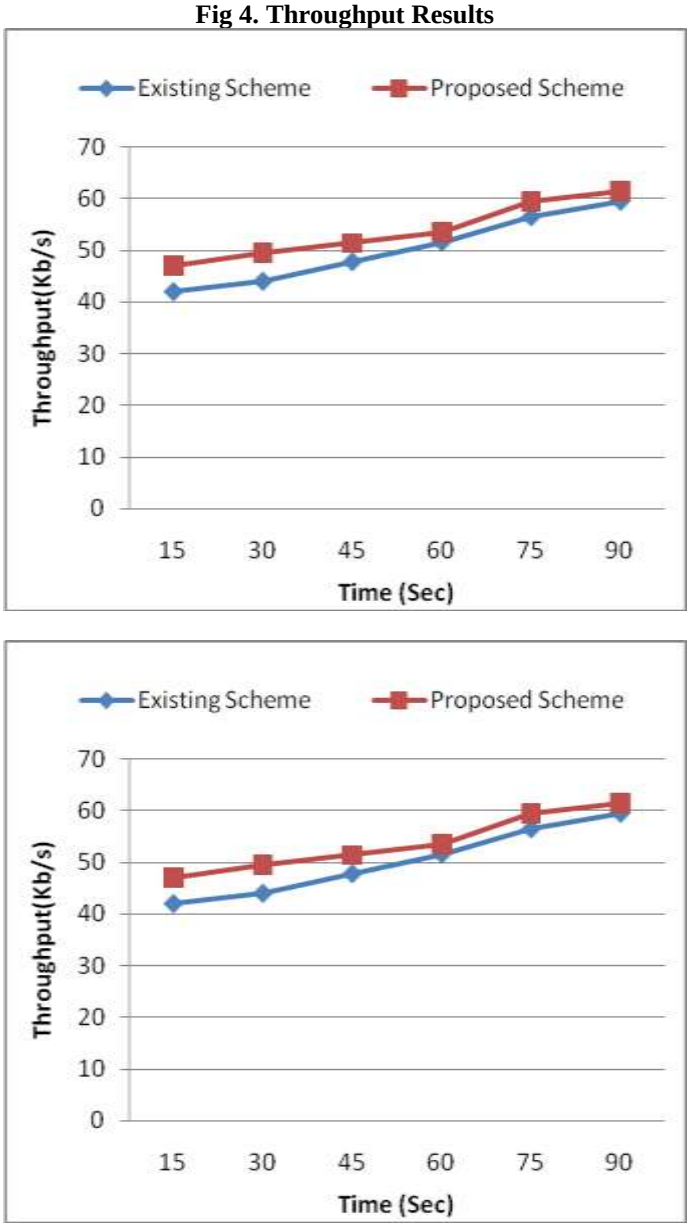
From the above table 1, analyzed that Four scale rating technique in the security mechanisms such as intrusion detection, network tolerance, redundancy rate, energy consumption, from these four method we have been attain increased than the existing one from the comparison, shows that, energy consumption is less than existing and other factors are very high due to proposed work.

Fig 3. Comparison Results



B. Throughput Comparison

Fig 4. Throughput Results



In Table 2, one can be noticed that the throughput of the proposed method is high. The proposed scheme can extensively advance the intrusion detection accuracy. As a result, the throughput of the proposed scheme is high which is easy to detect the network intrusion efficiently and its performance is superior to its rivals.

Table 2

TIME (sec)	Existing Scheme	Proposed Scheme
15	42	47
30	44	49.5
45	47.8	51.4
60	51.6	53.45
75	56.5	59.45
90	59.5	61.47

IV. Conclusion

Multipath routing helps in successful completion of the task in the heterogeneous networks, but identifying the malicious nodes between heterogeneous networks and surpassing them is often energy consuming and time-delayed. In order to overcome this, a real time system was formulated by identifying the Mean time to repair and the mean time between failures in multipath routing. When there are more than two nodes in the heterogeneous network are identified as malicious, the Mean Time to Repair is applied on the specific network so as to rely on the particular network's tolerance and once the decrease in mean time to repair is achieved the routing resumes with a delay time of acceptable mean time between failures. As this type of tolerance monitoring system helps network operators and server managed service providers to maximize security and an undisruptive process completion without any drop-offs, which can gain advantage in less energy consumption and reduce network compromises. This redundancy model ensures high life time of sensor networks, even intrusion tolerance system can be extended in the future work.

References

[1]. S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007.

[2]. A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L.B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 2005 ACM Workshop Quality Service Security Wireless Mobile Netw.

[3]. Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008 .

[4]. Philipp Hurni and Torsten Braun "Energy-Efficient Multi-Path Routing in Wireless Sensor Networks" 7th International Conference, September 10-12, 2008.

[5]. Jing Deng, Richard Han, Shivakant Mishra "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks" University of Colorado, Department of Computer Science Technical Report CU-CS-939-02.

[6]. Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks Hamid Al-Hamadi and Ing-Ray Chen, Member, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013 .

[7]. 'QoS Tradeoff Analysis of Multipath Routing Protocols for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks'; Hamid Al-Hamadi,Ing-Ray Chen, ISPA '12 Proceedings of the 2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications

[8]. Mohamed Mubarak T, Syed Abdul Sattar, G.Appa Rao, Sajitha M," Intrusion detection: An Energy efficient approach in Heterogeneous WSN,"in proc.2011 IEEE International Conference on Emerging Trends in Electrical and Computer Technology.

[9]. X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," in Proc. 2005 IEEE Veh. Technol. Conf., pp 2528-2532.

[10]. S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in Proc. 2003 Conf. IEEE Computer Commun., pp. 1713–1723

[11]. Simulation of Wireless Sensor Network Security Model Using NS2; Nayana Hegde, Dr.Sunilkumar S.Manvi, International Journal of Latest Trends in Engineering and Technology, 2014