Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.356 – 366

RESEARCH ARTICLE

PRIVACY AND ENERGY PRESERVING PARALLEL MACHINE INTELLIGENCE BASED WIRELESS SENSOR NETWORK WITH PATH RELOCATION

Miss. S.Rupitha*, Mrs. A.Sankareswari, M.C.A., M.Phil.******

*M.Phil(Computer Science), Research Scholar, Vivekanandha College for Women, Unjanai, Tiruchengode, India

******Assistant Professor in Computer Science, Vivekanandha College for Women, Unjanai, Tiruchengode, India

ABSTRACT: In WSNs (Wireless Sensor Network), how to conserve the limited power resources of sensors to extend the network lifetime of the network as long as possible while performing the sensing and sensed data reporting tasks, is the most critical issue in the network design. In many applications, the node closer to the Source and destination are overburdened with huge traffic load as the data from the entire region are forwarded through them to reach to the sink. In this project, the path relocation concept is used to reduce the delay and also to reduce the data loss in the network. By path relocation we can form the larger network. By using the Parallel Machine intelligence the actor nodes are created and it is used for the path selection during the process of communication. To increase the security in the network Modified RSA Algorithm is used. This algorithm is used to increase the security in the packet transfer during the process of communication in the network. As the result, it shows that the proposed method performs well when compared with the existing method in terms of security, loss and the delay factor. The performance analysis is done with the graphical representation

Keywords: RSA, path Relocation, Shortest path, WSN

1. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless network is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure

Wireless Sensor Networks (WSNs) have gained world- wide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user. Another concept in Wireless Sensor Network is Clustering, which means Grouping of similar objects or sensors in our context distance or proximity, Logical organizing.

A wireless sensor node is capable of gathering information from surroundings, processing and transmitting required data to other nodes in network. The sensed signal from the environment is analog which is then digitized by analog-to-digital converter which is then sent to microcontroller for further processing. While designing the hardware of any sensor node the main feature in consideration is the reduction of power consumption by the node. Most of the power consumption is by the radio subsystem of the sensing node. So the sending of required data over radio network is advantageous. An algorithm is required to program a sensing node so that it knows when to send data after event sensing in event driven based sensor model. Another important factor is the reduction of power consumption by the sensor which should be in consideration as well.

2. LITERATURE REVIEW

Hamza Rahmani, Nabil Sahli And Farouk Kamoun

The nature of the threats carried by Distributed Denial of Service (DDoS) attack requires effective detection as well as efficient response methods. However, feature-based schemes are unsuitable for real-time detection due to their complicated calculations and most of the statistical-based schemes do not distinguish DDoS attacks from legitimate changes. Besides, it is impossible to set a threshold that takes into account both false positives and false negatives. A hard threshold reduces the risk of false negatives but significantly increases the rate of false positives. In contrast, a soft threshold can easily be exploited by attackers to insert a malicious traffic that respects the conduct of good flow. To avoid these defects, we suggest a two-stage approach based on the detection of breaks in the distribution of connections size. A connection is defined as the aggregate traffic between two IP addresses, where one address belongs to the police address set, and the other is a foreign address. The connection size is measured in number of packets. To achieve our goal, we employ Total Variation Distance (TVD) to measure horizontal and vertical similarity among flows. We investigate a class of intelligent denial of service attacks which, unlike high-rate attacks, are difficult for other's schemes to detect. The experimental results indicate that our scheme can detect DDoS flooding attacks accurately. The effectiveness of our approach, even against intelligent attacks, is around 90%

Ashley Chonka, Jaipal Singh, And Wanlei Zhou

DDoS attack traffic is difficult to differentiate from legitimate network traffic during transit from the attacker, or zombies, to the victim. In this paper, we use the theory of network self-similarity to differentiate DDoS flooding attack traffic from legitimate self-similar traffic in the network. We observed that DDoS traffic causes a strange attractor to develop in the pattern of network traffic. From this observation, we developed a neural network detector trained by our DDoS prediction algorithm. Our preliminary experiments and analysis indicate that our proposed chaotic model can accurately and effectively detect DDoS attack traffic. Our approach has the potential to not only detect attack traffic during transit, but to also filter it.

Denial of service (DoS) attacks is designed to disrupt network services, by intentionally blocking or degrading the available resources used by them. One of the major problems for

DDoS detection methods is the difficulty of differentiating DDoS attack packets from legitimate packets, since attackers mimic their attack traffic amongst legitimate traffic in order to hide their attack.

3. METHODOLOGY

PARALLEL MACHINE INTELLIGENCE

Parallel Machine Intelligence is the intelligence exhibited by machines or software. Parallel Machine intelligence is used for many purposes; here it is used to find the nearest shortest path for several time periods. That process is carried out by using the Activators. The parallel Machine intelligence is acts as path fixer. The time periods are determined by the shortest path Algorithms. By the use of the parallel machine intelligence method the energy efficiency of the node is increased.

TOPOLOGY DISCOVERY

The topology is constructed based on the Top-Disc algorithm using our own path cost metric. For the Route Discovery process the request is sent by the source to the destination. And the Acknowledgement received by the source from the destination for the topology discovery process. Top-Disc Algorithm which is derived from the simple greedy log(n)-approximation algorithm for finding the set cover.

ROUTING ALGORITHM

Divide the whole region into several grids. These divisions are based on the transmission range of the sensor nodes. Routing Algorithm forms the general Structure to the network. The Route Request, Routing Reply, Demand factors are all controlled by the routing algorithm method.

AODV ROUTING PROTOCOL

In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to

the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

MODIFIED RSA ALGORITHM

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

The Modified RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime.

- *e* is released as the public key exponent. *e* having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of *e* (such as 3) have been shown to be less secure in some settings.

5. Determine *d* as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., *d* is the multiplicative inverse of *e* (modulo $\varphi(n)$).

- This is more clearly stated as: solve for *d* given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
- This is often computed using the extended Euclidean algorithm. Using the pseudo-code in the *Modular integers* section, inputs *a* and *n* correspond to *e* and $\varphi(n)$, respectively.
- *d* is kept as the private key exponent.

The *public key* consists of the modulus *n* and the public (or encryption) exponent *e*. The *private key* consists of the modulus *n* and the private (or decryption) exponent *d*, which must be kept secret. *p*, *q*, and $\varphi(n)$ must also be kept secret because they can be used to calculate *d*.

- An alternative, used by PKCS#1, is to choose *d* matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p - 1, q - 1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for *d*. λ can also be defined using the Carmichael function, $\lambda(n)$.
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that *p* and *q* match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key *d* secret. Bob then wishes to send message *M* to Alice. He first turns *M* into an integer *m*, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme.

Decryption

- Alice can recover *m* from *c* by using her private key exponent *d* via computing
- Given *m*, she can recover the original message *M* by reversing the padding scheme.

In practice, there are more efficient methods of calculating c^d using the pre-computed values.

4. EXPERIMENTS AND RESULTS

In this project, the path relocation concept is used to reduce the delay and also to reduce the data loss in the network. By path relocation we can form the larger network. By using the Parallel Machine intelligence the actor nodes are created and it is used for the path selection during the process of communication. To increase the security in the network Modified RSA Algorithm is used.

This algorithm is used to increase the security in the Packet transfer during the process of communication in the network. As the result, it shows that the proposed method performs well when compared with the existing method in terms of Security, Loss and the delay factor. The performance analysis is done with the graphical representation.

To increase the security in this network we proposed the Modified RSA Algorithm. By using this proposed algorithm the parameters of the network is increased. The life time of the individual node is increased by that the energy efficiency of the network is increased. The comparison shows that the proposed method performed well when compared with the existing method.

The figure1 which represents the difference between the existing algorithm and the proposed algorithm with parameters cost, efficiency and accuracy**.** The figure2 which represents the difference between the existing algorithm and the proposed algorithm with Energy Efficiency and the Time Period. The X-axis represents the Time and the Y-axis represents the energy efficiency of the network.

RESULTS AND COMPARISON

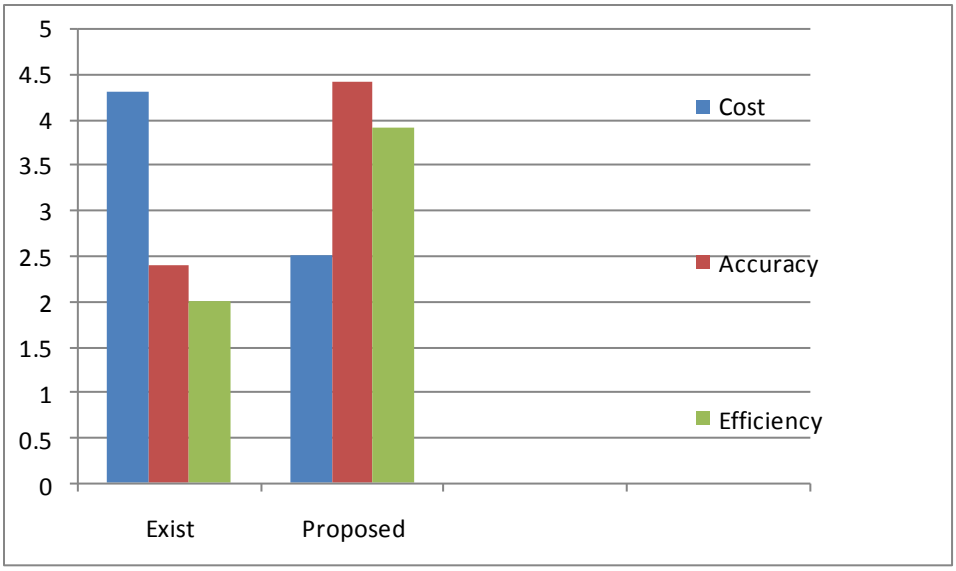

Fig 4.1 Parameter cost, Efficiency and Accuracy

The figure which represents the difference between the existing algorithm and the proposed algorithm with parameters cost, efficiency and accuracy**.**

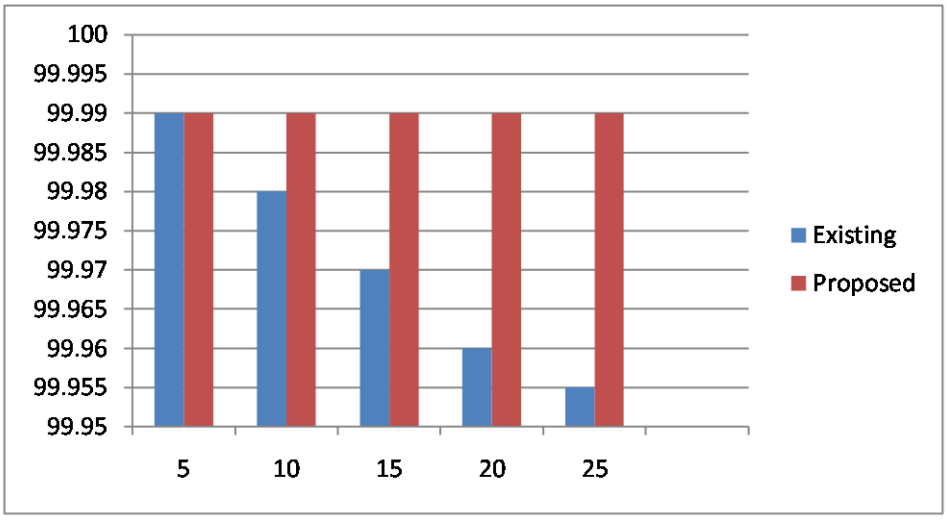

Fig 4.2 Energy efficiency VsTime Period

The figure which represents the difference between the existing algorithm and the proposed algorithm with Energy Efficiency and the Time Period. The X-axis represents the Time and the Y-axis represents the energy efficiency of the network

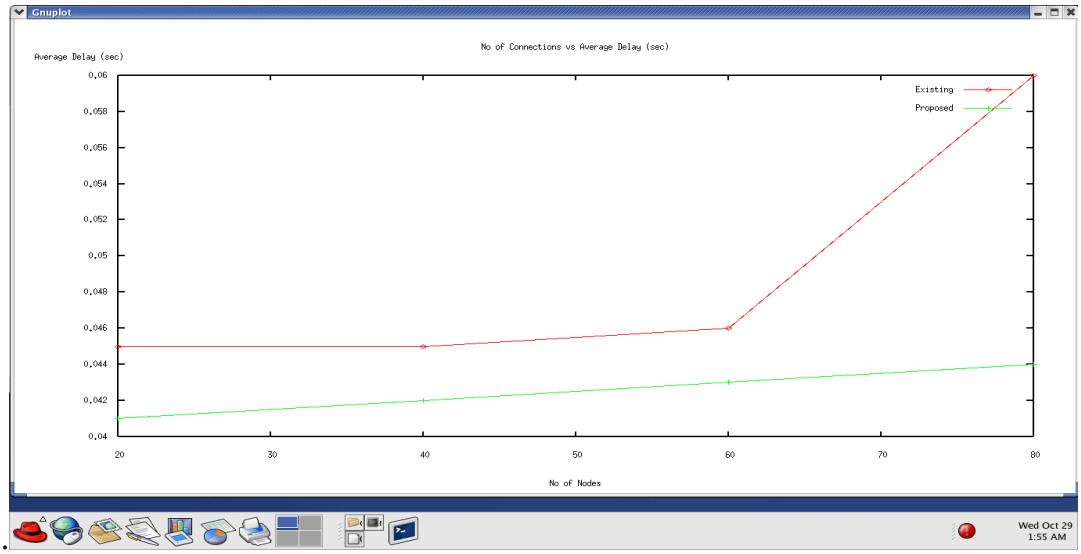

Fig 4.3 Number of nodes Vs delay factor

The comparative analysis of the existing and the proposed method is given. The Parameters are the Number of nodes Vs delay factor. The Graphs shows that the proposed method produce less delay when compared with the existing method.

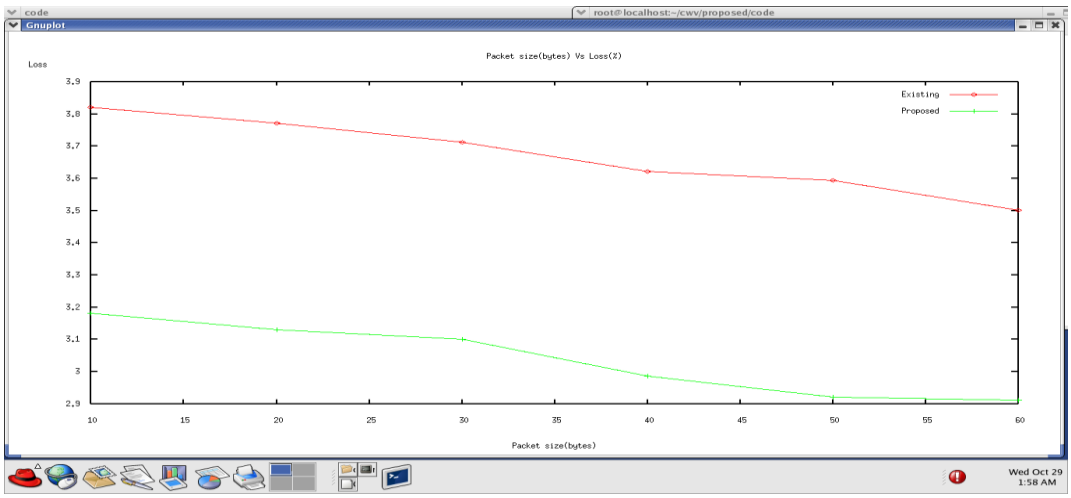

Fig 4.4 Packet Loss Vs Loss Factor

The comparative analysis of the existing and the proposed method is given. The Parameters are the Packet size and the loss factor. The Graphs shows that the proposed method produce less loss when compared with the existing method

5. CONCLUSION AND FUTURE ENHANCEMENT

In many applications, the node closer to the Source and the destination are over burdened with huge traffic load as the data from the entire region are forwarded through them to reach to the sink. Proposed the routing algorithm for path relocation. By path relocation we can form the larger network and the accuracy factors are very low in this kind of network. By using the Parallel Machine intelligence the actor nodes are created and it is used for the path selection during the process of communication. The life time of the individual node is increased by that the energy efficiency of the network is increased.

The future work is to increase the Quality of service parameters and prefer the performance analysis between the several protocols like DSR, DSDV and AOMDV protocols. And in the networks the main disadvantages is that the lack of Strong Authentication and Cooperation. The network lost its security by the active attacks and the passive attacks which were created by the external environment. So the future enhancement is to provide strong intrusion detection in the network by the help of several algorithms and also by the Artificial intelligence. And also to increase the control in the network the concept of cooperation is enhanced for the future work.

REFERENCES

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS denfense mechanisms,"ACM SIGCOMM Computer Commun. Rev.,vol. 34, no. 2, pp. 39–53, 2004.
[2] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in Proc. 2005 Conference on Applications, Technologie, Architectures and Protocols for Computer Communications,pp. 217–228.
[3] A. Ziviani, A. Gomes, M. Monsores, and P. Rodrigues, "Network anomaly detection using nonextensive entropy," IEEE Commun. Lett., vol. 11, no. 12, pp. 1034–1036, 2007.
[4] H. Rahmani, N. Sahli, and F. Kamoun, "DDoS flooding attack detection scheme based on F-divergence,"Computer Commun., vol. 35, no. 11, pp. 1380–1391, 2012.
[5] A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks,"IEEE Commun. Lett., vol. 13, no. 9, pp. 717–719, 2009.

[6] G. Carl, G. Kesidis, R. R. Brooks, R. Richard, and S. Rai, "Denial-ofservice attack-detection techniques,"Internet Computeing, vol. 10, no. 1, pp. 82–89, 2006.
[7] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 412–425, Mar. 2011.
[8] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Trans. Inf. Forensics and Security, vol. 6, no. 2, pp. 426–437, June 2011.
[9] Y Chen, X. Ma, and X. Wu, "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory,"IEEE Commun. Lett., vol. 17, no. 5, pp. 1052–1054, 2013.

