International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 19 Issue 2 – JANUARY 2016.

RELIABLE AND ENERGY-SAVING FORWARDING TECHNIQUE FOR MANET USING MULTIPATH ROUTING

S.Poonthalir[#1], Mrs.S. Hema[*2]

[#1]*M.Phil.,Scholar PG& Research Department of Computer Science,*
[*2]*M.C.A.,M.Phil., Assistant Professor, PG& Research Department of Computer Science*

***Abstract*--Wireless Sensor Network generally deployed in natural environment, so large number of security issues are there. Protect the data in WSN require approaches that will make data transmission more secure from the attackers. Data transmission can be performed based on cluster using imperialist competitive algorithm. It can divide the cluster in tosub-clusters and compete with each other until one of these cluster nodes is selected. ECAES algorithm is used for efficient data transmission to exploit key selection from elliptic curve as an abelian group with points as elements. To avoid fake identities in packet transfer,the different approach called fake agent attackers is used which prevent the traffics and fake distinctiveness of nodes located at communication range around target area. Energy efficiency can be improved by using Adequate energy which select the most appropriateneighbor node with position closeness and substitute node isnot only required to be close to the faulty node to ensure the sensing accuracy, butalso have higher residual energy to guarantee further stability. So the effective utilization of algorithm is used to reduce dropping ratio and minimize overhead.**

Keywords: WSN, Adequate energy, ECAES, fake agent attackers, Imperialist Competitive algorithm

I. INTRODUCTION

Wireless Sensor Network In wireless communications have enabled low cost, low-power, multifunctional sensor nodes for the development that are small size and short distances communication. The sensor networks used tiny sensor nodes, which consist of sensing, data processing, and communicating components. A sensor node is a node in a wireless sensor network that is capable of performing rarefaction, sensory information for congregation and communicating with other consecutive nodes in the network. Wireless sensor Network is connected with algorithms and set of protocols for efficient communication to connecting the nodes.The energy efficiency provided adequate energy that select the neighbor node also close to faulty node and stable residual energy for reducing the dropping packets.

The problem consists of monitoring a set of targets in a designated geographical area to a satisfactory level for packet dropping it is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It may also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. It may also modify the data it generates to protect itself from being identified or to accuse other nodes. A detection technique is to detect unauthorized or unusual behavior in a network, Intrusion Detection System and node monitoring techniques are used for detection. The attacker knows the minimum misbehavior threshold and if they can manipulate the packet dropping rate, it becomes difficult to detect the misbehaving node. The Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively used information gathering, eavesdropping or actively used harmful packet forwarding, packet dropping, and hole attacks. The packet dropping and modification is a main problem to overcome that used another attack to prevent the loss in packet. The schemes effectively detecting the dropping packets, low communication and energy overheads, being compatible problem in the dropping or loss among packet through mitigate the attacks. The packet dropping is used filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. The node categorization algorithm to identify nodes that are packet droppers for sure, suspicious packet dropper’s problem in traffic rate and static only.

To overcome these problem use fake agent attackers, a huge number of identities are forged and fake identities are created by the malicious nodes in the network to avoid the fake distinctiveness. To divide the cluster into sub cluster by using Imperialist Competitive Algorithm(ICA) is one of the most powerful algorithms; it has been used extensively to solve different kinds of optimization problems. In this ECAEC is modern technique for encoding and decoding purpose. The various energy sources having different methodsis more sufficient, in adequate energy to improving the energy efficiency that to selected the nearby node with hurler position. In Substitute node not only required be close with faulty node but also sensing accuracy is ensure, after select the cluster header use ECAES Algorithm to select a key, to identify the fake agent attackers by using this algorithm.

Architecture Diagram for Proposed System:

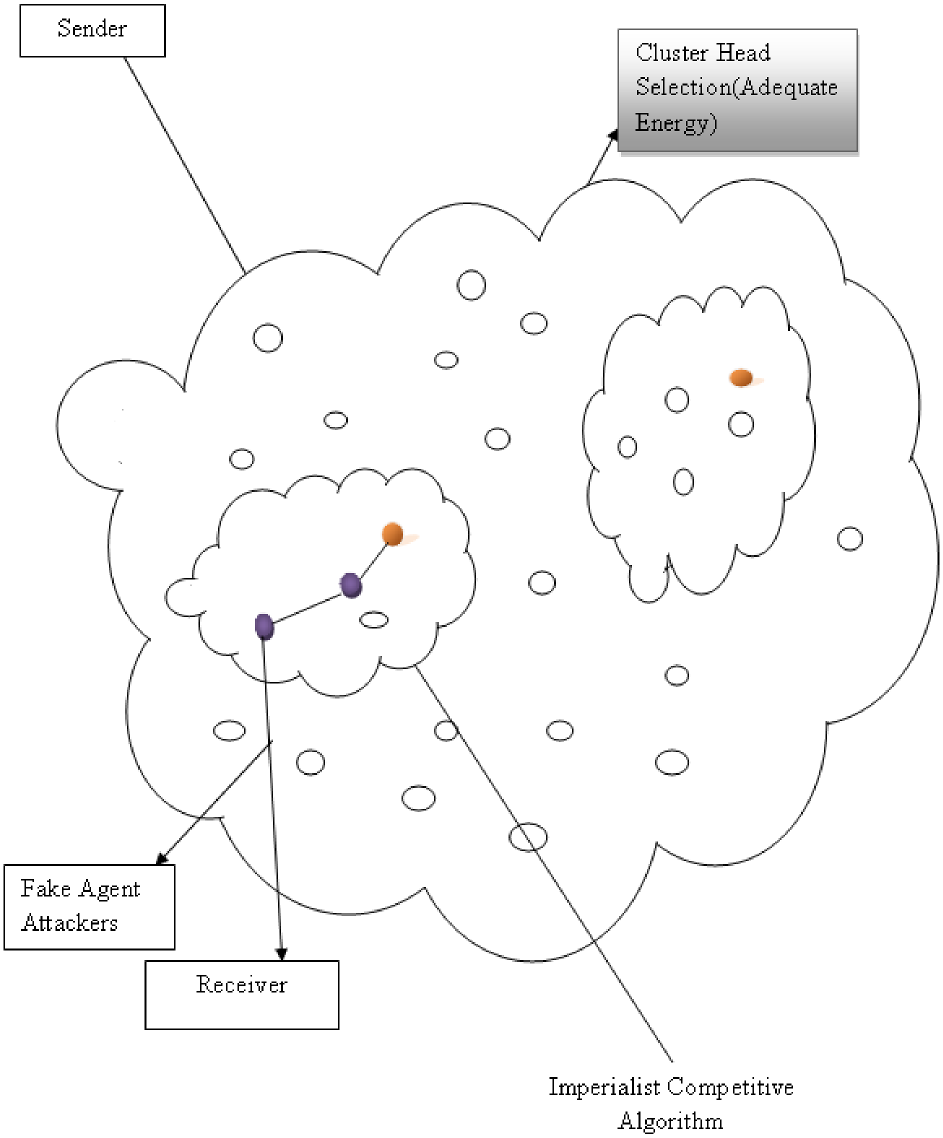
Sender
Cluster Head Selection(Adequate Energy)
Fake Agent Attackers
Receiver
Imperialist Competitive Algorithm

Figure 1.Architecture Diagram

The sender selects the node by using the ECAES Algorithm, the cluster can be divided into sub cluster and the sub cluster will select the cluster head. After select the cluster header use ECAES Algorithm to select a key, to identify the fake agent attackers by using this algorithm. The adequate energy can analysis the energy efficiency to select the closer position node, after select the node by using Imperialist Competitive Algorithm to find the shortest path and to send the data to the receiver.

II. LITERATURE SURVEY

In paper [1],MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-hop Wireless Ad Hoc Network is introduced. Local monitoring as a powerful technique for mitigating security attacks in multi-hop ad-hoc networks. In local monitoring, nodes overhear partial neighborhood communication to detect misbehavior such as packet drop or delay. Local monitoring is vulnerable to a class of attacks called stealthy packet dropping. Stealthy packet dropping disrupts the packet from reaching the destination by malicious behavior at an intermediate node. The malicious node gives the impression to its neighbors that it performed the legitimate forwarding action. A legitimate node comes under suspicion, four ways of achieving stealthy packet dropping, none of which is currently detectable and provides a protocol called MISPAR based on local monitoring to remedy each attack. These techniques having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor.

In paper [2],LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks is used. Preventive mechanisms can be applied to protect them from an assortment of attacks. More sophisticated methods like intrusion detection systems are neededto achieve a more autonomic and complete defense mechanism, even against attacks that have not been anticipated in advance. A lightweight intrusion detection system, called LIDeA, designed for wireless sensor networks. LIDeA is based on a distributed architecture, in which nodes overhear their neighboring nodes and collaborate with each other in order to successfully detect an intrusion.

In paper [3],Reputation-based Framework for High Integrityincrease in automatic data collection capabilitiesthrough efficient deployment of tiny sensing devices.This will allow users to measure phenomena of interest at unprecedented spatial and temporal densities. Data integrity is vulnerable to both node and system failures. Indata collection systems, faults are indicators that sensor nodes are not providing useful information. The data fusion systems the consequences are more; the outcome is easily affectedby corrupted sensor measurementsthat allow the sensor nodes to develop a community of trust. This framework each sensor node maintains reputation metricswhich both represent past behavior of other nodes and are used as an inherent aspect in predicting their future behavior.

In paper [4], Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-Dimensional Trust Management Approach is used.Nodes in Mobile Ad hoc Networks (MANETs) are required to relay data packets to enable communication betweenother nodes that are not in radio range with each other. For selfish or malicious reasons, a node may fail tocooperate during the network operations or even attempt todisturb them, both of which have been recognized as misbehaviors. Various trust management schemes have been assess the behaviors of nodes so as to detect and mitigatenode misbehaviors in MANETs. It describes a multi-dimensional framework to evaluate the trustworthiness of MANET node from multiple perspectives. This scheme evaluates trustworthiness from threeperspectives: collaboration trust, behavioral trust, and referencetrust. The different types of observations are used to independentlyderive values for these three trust dimensions.

In paper [5], Packet-dropping Adversary Identification for Data Plane Security, the design of packet dropping adversary identification protocols those are robust to both benign packet loss and malicious. A secure and practical packetdropping adversary localization scheme that is robust andachieves a high detection rate and low communication andstorage overhead – the three key performance metrics forsuch protocols in realistic settings. Other recent work justoptimizes either the detection rate or the communicationoverhead.For design spaceof acknowledgment based protocols to identify a packet dropping adversary on a forwarding path, a set of basic protocols, each simplifying a design dimension, the underlying tradeoff between theperformance metrics. For each basic protocol, we presentboth upper and lower performance bounds via theoreticalanalysis, and average-case.

In paper [6], Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using two-hop Neighbor Knowledge Selective forwarding attack is one of the easiest implement and damaged attacks in multi-hop routing protocols. A lightweight detection algorithm based only on the neighborhood information, the detection algorithm can detect selective forwarding attack with high accuracy and little overhead imposed on detection modules than previous works.For detection modules consume less energy than previous works by using over-hearing mechanism to reduce the transmission of alert packets.A sensor node is more constrained in resources as compare to ad hoc node thus it is impossible to apply detection techniques in wired or ad hoc networks.

In paper [7], Reputation and Trust-based Systems for Ad Hoc and Sensor Networkscan make reputation and trust guided decisions, in choosing relay nodes for forwarding packets for othernodes, or for accepting location information from beacon nodes. This not only provides MANETs and WSNs with the capability of informed decisionmaking, but also provides them security in the face of internal attacks where cryptographic security gives way. The way in which a system discovers, records, andutilizes reputation to form trust, and uses trust to influence behavior is referred toas a reputation and trust-based system. This dedicated to providing thereader with a complete understanding of reputation and trust-based systems fromthe wireless communication perspective.

In paper [8], Protocols and Lower Bounds for Failure Localization in the Internetprove lower bounds for such protocols every secure FL-PQM protocol requires each intermediate node onthe path to have some shared secret information (e.g. keys).If secure FL-PQM protocol exist then so do one-way functions.Every black-box construction of a FL-PQM protocol from a randomoracle that securely localizes every packet and adds at most

O(log n)messages overhead per packet requires each intermediate node toinvoke the oracle. That implementing FL-PQM requires active cooperation (i.e. maintaining keys and agreeing on, and performing, cryptographic protocols) from all of the intermediate nodes along the path. This may be problematic in the Internet, where links operate at extremely high speeds, and intermediate nodes are owned by competingbusiness entities with little incentive to cooperate.

In paper [9], Insider Attacker Detection in Wireless Sensor Networks, the destructive to network functions, insiderattackers are not detectable with only the classic cryptography basedtechniques. Many mission-critic sensor network applicationsdemand an effective, light, flexible algorithm for internaladversary identification with only localized information available.The insider attacker detection scheme proposed in this papermeets all the requirements by exploring the spatial correlationexistent among the networking behaviors of sensors in close proximity.

It is exploratory in this algorithm considers multiple attributes simultaneously in node behavior evaluation, with no requirement on aprior knowledge about normal/malicious sensor activities. This algorithm is purely localized, fitting well to the large-scale sensor networks that internal adversaries can be identified with a high accuracy and a low false alarm rate when as many as 25% sensors are misbehaving.

III. METHODOLOGIES IN PROPOSED SYSTEM

ECAES Algorithm

Encryption and Decryption can done by using Elliptic Curve Authenticated Encryption Scheme (ECAES) or simply called elliptic curve Encryption Scheme, this algorithm is a deviationof public-key encryption. ECAES encryption for certain data integrity and authentication, use session keys (symmetric keys) for data encryption, Session keys are exchanged using ECAES encryption. To authenticate the nodes and generate session keys between the nodes and the sink, in between the nodes need to communicate. Public key Encryption is support for semantic security. The Elliptic Curve Authenticated Encryption Schemeto encrypt the message to select the random numbers,for clusterdivide into two sub clusters by using ICA and form a sub cluster to select the cluster head thatselect the key by using ECAES Algorithm.To decrypt a cipher text toperform a key validation on check, verify,compute the Keys. To encrypt the message by using the symmetric key encryption algorithm and to

It is anefficient encryption scheme which provides semantic security against towards allowed usingAlice and bob. The security of the scheme is based on the ECAES algorithm. Two IES are standardized are Discrete Logarithm Integrated Encryption Scheme (DLIES) and Elliptic Curve Integrated Encryption Scheme (ECIES), which is also known as the Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme. Alice can encrypt and bob can decrypt the message by using the efficient ECAES algorithm the optional sharing information also available to share the message.

Public key possesses not only confidentiality but also characteristics like enforceability and non repudiation. An efficient key management scheme based on public key elliptic curves cryptography scheme for Heterogeneous Sensor Networks, it is optimized for cluster sensor networks and is efficient in terms of complexity, number of message exchange, computation, and storage requirements with optimized security benefits for clustered environment. The key management possesses not only confidentiality but also characteristics like enforceability and non repudiation.The ECAES Algorithm have efficient key management scheme for exchange message to compute a different security measures.

Imperialist Competitive algorithm

Imperialism is the procedure of spreading the control of an imperial beyond its own limits in a cluster. An imperialist managethe network by direct rule or by less control of arcadeto divided cluster using adequate energy. This algorithm is used to find the adequate energy of wireless sensor network to detect in efficient way for using this algorithm.To divide the cluster into sub cluster by using Imperialist Competitive Algorithm(ICA) is one of the most powerful algorithms; it has been used extensively to solve different kinds of optimization problems.

Each group of the node is called a sub cluster; some of the sub cluster in the nodes is selected to be the imperialist. The node has encountered the selectedneighboring to the task, the node has better range and algorithm has efficiently utilized the clusters.All the networks of initial node are divided among the imperialists based on their function for instance and choosing cluster head having adequate energy remaining sub cluster nodes are cluster child. The Network in each of domain starts moving toward their relevant position and changes the place in the new one. The control of each sub cluster is made up of imperialist require function and networks. It is based on cluster control. The cluster which is weaker than the others, loses its networks until there will be no network in that. This action is extinction of the weakest cluster, its imperialist is considered as the bestNetwork. The level of imperialist Challenges is when there is only one domain is the optimum point.ICA can provide more accurate solutions in less computational time when compared to the coverage, energy-efficient control algorithm and improved the cluster energy.

REFERENCES

[1] Khalil and S. Bagchi, “MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. Netowrks (SecureComm ’08), 2008

[2] Krontiris, T. Giannetsos, and T. Dimitriou, “LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. Netowrks (SecureComm ’08), 2008.

[3] S. Ganeriwal, L.K. Balzano, and M.B. Srivastava, “Reputation-Based Framework for High Integrity Sensor Networks,” ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37, 2008.

[4] 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.

[5] X. Zhang, A. Jain, and A. Perrig, “Packet-Dropping Adversary Identification for Data Plane Security,” Proc. ACM CONEXT Conf. (CoNEXT ’08), 2008

[6] T.H. Hai and E.N. Huh, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge,” Proc. IEEE Seventh Int’l Symp. Network Computing and Applications (NCA ’08), 2008.

[7] Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, “Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks,” Proc. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2008

[8] Barak, S. Goldberg, and D. Xiao, “Protocols and Lower Bounds for Failure Localization in the Internet,” Proc. Eurocrypt, 2008.

[9] F. Liu, X. Cheng, and D. Chen, “Insider Attacker Detection in Wireless Sensor Networks,” Proc. IEEE INFOCOM, 2007.