International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.5., Issue.2, 2017
March-April

RESEARCH ARTICLE

ISSN: 2321-7758

PREVENTION OF MALICIOUS NODE IN LTE NETWORK

S.SURYA[1], P. KARTHIKEYAN[2]
[1]PG Scholar, [2]Professor & Head
[1]P.G Scholar, Department Of Computer Science and Engineering, M.E-Computer Science Engineering,
Anna University Bit Campus, Trichy, Tamilnadu, India
Email:yessurya7@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering,
Anna University Bit Campus, Trichy, Tamilnadu, India

S.SURYA

ABSTRACT

Fundamental security elements in wireless sensor systems is the authentication procedure performed by means of the subscriber identity module .different problem such as routing attacks, security branch problem, one among them is malicious node attack. The malicious node attack is an active attack which causes severe damage to the network. The proposed work we introduce a new kind of authentication that the proposed algorithm is most effective to epilation of malicious node.

Key Words:–Network security, LTE, Malicious node, Dynamic node.

1. INTRODUCTION

Wireless based on cellular networks is one of the most successfully deployed technologies of the last ten years and coverage of cellular networks in the world has generally become pervasive. Both an effect and a cause of this success may be seen n in the evolutional cycle of the network technologies. Flea group algorithm (FGA) is widely used for route optimization in WSNs. Kassabalidis et al. propose the typical route Ant-Net algorithm [1], which only considers an optimal route and minimizes energy consumption to a great amount, this leads to a large number of ants on the shortest route, and results in too fast energy consumption on the optimal route and node death. Thus life cycle of the entire network is reduced. T Camilo et al. give the Improved Ant-Based Routing (IABR) and Energy Efficient Ant Based Routing (EEABR) algorithms [2]. They build a new function to calculate pheromone left by the backward ants on their way home, but the algorithm doesn't consider energy balance of the entire network. This is extremely important to the wireless sensor network. Luo Xu et al. come up with the improved ant colony algorithm based on [3], named OARA [4]. The algorithm introduces the penalty function and dynamic weight factor in the transition probability formula, and applies the combination of local and global pheromone to update route information

In this scenario, mobile communication networks have gained the role of critical infrastructure for the global community like electricity or transportation so that many individuals and business activities relying on them for their everyday operations may be severely impacted by any service disruption or degradation . It is thus critical to tackle the problem of security in mobile networks from every possible perspective, not only focusing on the confidentiality and integrity of codes [5], end-to-end connections [6], [7], information flows [8] but also considering the availability of the network itself.

2. LONG TERM EVOLUTION

LTE network has is built using packet switched backbone and core network using end to end IP connectivity. LTE operates in lower 700 MHZ and upper bands of 1700/2100 MHZ frequencies. 4G LTE service providers in the US, AT&T, TMobile and Verizon operate using both lower and upper bands. LTE supports both the versions of duplexing (i.e.,transmit and receive) methods Time-Division Duplexing (TDD), and Frequency-Division Duplexing (FDD) combined with the downlink modulation scheme, Orthogonal Frequency Division Multiple Access (OFDMA) to achieve maximum peak downlink data rate of 100 Mbps In Frequency-Division LTE (FD-LTE), a pair of separate frequencies will be used for transmission and reception. In Time-Division LTE (TD-LTE), a single frequency will be used with time-split to transmit and receive using the same frequency carrier. Uplink transmission uses Single-Carrier Frequency Division Multiple Access (SCFDMA) to achieve maximum throughput of 50 Mbps using 20 MHZ bandwidth [4]. A scalable bandwidth of 20 MHZ from 1.4 MHZ, 3 MHZ, 5 MHZ, 10 MHZ and 15 MHZ along with faster response time thanks to the high data rate, unlike its previous cellular counterparts, enables LTE to out swim the contemporary 4G technology choices. The LTE provides a migration path for GSM and CDMA based operators by facilitating the convergence of wireless technology. The primary goal of this new technology is to improve spectral efficiency, bandwidth and throughput by means of deploying cost effective network elements using open standards with improved data and application services for the end users. It is expected to support lower latency, high level of security, to support different Quality of Service (QoS) [3]. The heartening part of the LTE network architecture is the Evolved Packet Core System (EPS) architecture as outlined system consists of the following two major components:

(i) EPC Core Network with Evolved Packet Core Network System Architecture Evolution (EPC/SAE) and

(ii) The new Radio Access Network (E-UTRAN). The Evolved UMTSRAN (E-UTRAN) is from the original 3GPP UMTS radios NodeB base station system. Evolved NodeB (eNodeB) works in LTE and as well co-exists with the GSM and UMTS network to support fallback procedures. EPC forms the main part of Core Network (CN).

3. EXISTING SYSTEM

3.1 Proactive secure-Aware Routing

With table-driven routing protocols, every node attempts to maintain consistent up to date information of routing to every existing node in the network. This is done in response to modifies in the network by having ideal node update its routing table and propagate the updates to its nearby nodes. Thus, the route is already known that the proactive in the wireless that when a packet needs to be forwarded and can be immediately used. the case for wired networks, the routing table is constructed using either distance vector or link-state algorithms containing a table of all the sink node, the next hop, and the number of hops to each destination. The DSR is a reactive routing protocol designed specifically for use in multi-hop wireless ad hoc networks of cellular nodes. In this protocol each source determines the route to be used in transmitting its packets to selected destinations. There are two main components, called Route Discovery and Maintenance. Route Discovery is the mechanism by which a node wishing to send a packet to a end user node obtains a path to the destination. Route Maintenance is the mechanism by which a node detects a break in its source route and obtains a corrected route. The source node knows the complete hop by hop route to the destination. The protocol allows multiple routes to any end-user node and allows each sender to select and control the routes used in routing its packets for use in load balancing or for increased robustness.

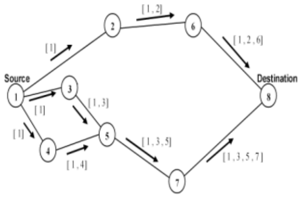

Figure 3.1 : Route Discovery.

The most direct interruption against a routing protocol is to aim the information of routing exchanged between nodes. By replaying routing information spoofing or altering, adversaries may be able to develop routing loops, repel or attract network traffic, shorten source or extend routes, generate spoofed error messages, dividing the network, to maximize end-to-end latency, etc. Several wireless sensor network routing method rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can false link layer acknowledgments for overheard packets addressed to nearby nodes. Goals include convincing the source node sender that a weak link is strong or that a dead or inactive node is alive.

3.3 MHRM (minimum hop routing model)

Energy efficient routing protocols for MANET try to minimize energy consumption by means of an efficiency of energy routing metric, used in routing table list computation instead of the minimum-hop metric. This way, a routing protocol not much difficult introduce energy efficiency in its packet forwarding. These protocols try either to route data through the path with maxi energy bottleneck, or to mini the end-to-end transmission energy for packets, or a giving weighted combination of both. A first approach for energy-efficient routing is known as Minimum Transmission Power Routing . That mechanism uses a simple energy metric, represented by the net energy consumed to forward the information along the route. This way, MTPR minimize the total transmission power consumed per packet, but it does indirectly affect the lifetime of each node. However, minimizing the transmission energy only differs from shortest hop routing if nodes can adjust transmission power levels, so that multiple short hops are more advantages, from an energy point of view, than a single long hop.

4. RELATED WORKS

Security is a critical issue for sensor systems sent in threatening situations, for example, military front lines. The ease prerequisite blocks the utilization of alter safe equipment on little sensor hubs. Henceforth, sensor hubs conveyed in open ranges can be traded off and used to complete different assaults on the system. In this paper, we consider the impact assault that can be effectively dispatched by a traded off (or threatening) malicious : a bargained malicious does not take after the medium access control convention and cause crashes with neighbor transmissions by sending a short network bundle. This assault does not find much vitality of the aggressor but rather can bring about a considerable measure of disturbances to the system operation. Because of the remote show nature, it is not trifling to recognize the assailant. In this paper, we propose a conveyed plan that depends on minimal effort equipment and can adequately GLM (Generalized linear Models). Our plan depends on breaking down physical-layer Received Signal Strength Index (RSSI) readings. We demonstrate that right recognizable proof of an antagonistic MALICIOUS can be accomplished with more prominent than 85% precision. We assist exhibit a strategy that debases effortlessly as the foundation commotion increment.

4.1. Detecting the malicious data overhead security

To counter the developing risk of wireless communication network subversions to the outline of a path, there is an requirement for straightforward, computerized techniques for identifying such has changes. In view of the reception of the Property Specification Security (PSS) for behavioral confirmation, and the coming of devices for consequently producing synthesizable builds for checking a PSS declaration, we propose another strategy called Security Checkers, which utilizes security-cantered PSS affirmations to make equipment plan units for identifying malicious considerations at runtime. We depict the procedure stream for making Security Checkers and exhibit by case how they can be utilized to identify attacker incorporations in a processor plan. Since the checkers can be utilized as a part of recreation, security, or as a feature of a manufactured outline, we represent how this procedure can be utilized to recognize malicious incorporations over a much more extensive portion of the processor advancement lifecycle, contrasted with existing strategies.

T-model convolution kernel consists of lower four parameters of the cross-model, similarly the inversed T-shaped model convolution kernel is composed of the upper four parameters. In the proposed image scaling algorithm, T-shaped and inversed T -shaped model filters are used for improving the quality of the images simultaneously. This efficiently minimizes the complexity of the convolution filter and greatly reduces the memory requirement from two to one line buffer for each convolution filter. Both the models gives the less area, less complexity and not more memory-needed convolution kernels for the enhance spatial and clamp filters to integrate VLSI chip of the proposed low-cost image scaling processor. General class of linear models that are made up of 3 technique : Random, Link Function and Systematic.

Random component: Identifies dependent variable (Y) and its probability distribution

Systematic Component: Identifies the set of explanatory variables (S1,...,Sk)

Link Function: Identifies a function of the mean that is a linear function of the explanatory variables.

5. PROPOSED SYSTEM

The proposed algorithm is based on the New way define the flea group optimization algorithm which helps to probability of path from source to sink node additionally game theory which aims at distributing the resources fairly among classes and detecting unwanted activities in network . Afterwards, the users with tightest delay requirements are served first by a novel queuing delay algorithm. Defined a actual firm provision to control scheduling process in LTE network. Instead, they defined nine classes with their corresponding Quality of Services (QoS) requirements. The first four classes are Guaranteed Bit Rate (GBR) and the other six classes are Non-GBR. Game theory was proposed in economics detecting distrube node where a group of players form a coalition to distribute the joint profits among their coalition.

The lifetime of the wireless node depends on too extent on the battery life, and the unreasonable energy consumption will cause the network to die prematurely and reduce the network lifetime. So how to design the WSN routing algorithm which can save node energy and improve the quality of network communication is the key point for WSN. FGO is widely used for route optimization in WSNs. the typical route linear method which only considers an optimal route and minimizes energy consumption to a great amount, this leads to a more number of ants on the shortest route, and results in too fast energy consumption on the optimal route and node death. Detection of malicious node initial step towards prevention

5.1 S2S Random - Conditionally process Normally distributed response with constant standard 15 deviation - Regression models fit so far.S2S Random has malicious distribution and it's model is called Logistic Regression. Count data (number of times in fixed area and/or taken of time)-S2S Random has Poisson distribution and it's model is called Poisson Regression When Count data have V(Y) > E(Y), model fit can be Negative Binomial Regression Continuous data with skewed distribution and variation that increases with the mean can be modelled with a Gamma distribution.

5.2 Systematic Component Response - Presence/Absence of characteristic Predictor - Numeric variable observed for each case Model - p(x) Probability of presence at predictor level x b1 = 0 P(Presence) is the same at each level of x b1> 0 P(Presence) increases as x increases b 1< 0 P(Presence) decreases as x increases.

$$s = \frac{e^{\beta_0} + k}{1 + e^{\beta_0 + \beta_1 x_1 + \cdots + \beta_k x_k}}$$

5.3 linear C flow function - A cellular network communication is a group of spatially distributed, independent devices that collect data by measuring physical or environmental conditions. Some of the conditions being measured are position, pressure, sound, moisture, temperature , usage information, and lighting. These referance, in the form of file like data, which can be pass through network, are conjution and grouped, and then send to the sink node.

Cellular network communication technique have been used for many applications like electricity system controls , industrial process control and human health monitoring. Traditionally, these cellular network tend to need a bits of energy to function, but decreasing the power needs of the system 16 developing the lifetime of the sensor devices, and creates space for battery energy applications .Battery-powered devices allow for wide-ranging use cases and opens opportunities for lower-ROI application number of pixels having the width of the original image and N is the number of pixels corresponding to the length of the original image.

IP Spoofing is the total number of intersection point corresponding to the size of the original image. New kind internet protocol fake is a method used to improve unauthorized access to node, whereby an interpreter illicitly entered another node in ideal network by controlling IP packets. IP fake involves alter the packet header with a spoofed sender IP address, the order value , and a checksum A spoofing attack is when a malicious party entered in to another device or operaters on a network in order to launch single step towards malfunction against network hosts, , spread malware, steal data or bypass access controls..

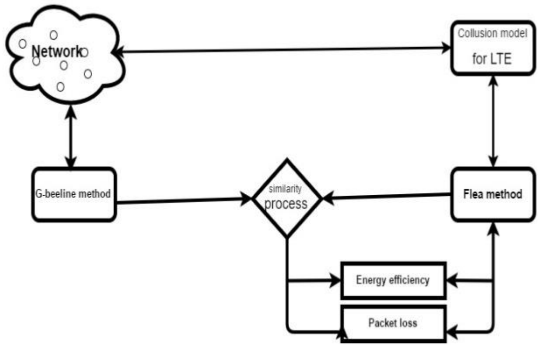

Fig 5.1 Architecture of prevention of malicious node

6. CONCLUSION

Due to their generic structure and, versatile field programmable open arrays allow dynamic again configuration of their logical resources just by configuration of loading files. However, this adaptable also opens up the danger of theft of intellectual property since these configuration of files can be easily cloned and extracted. In this context, the ability to tie a configuration to a selected device is an important step to intercept product counterfeiting. In this paper, we present a novel idea to identify and authenticate applications using intrinsic, device-specific information (also known as physically unclonable functions). Our terminal is based on the result of intentionally induced non oral collisions in synchronous di-port block RAM (BRAM). We show that the output of such write collisions can be used to form ideal machine signatures. In following to applications for chip detection and trusted, we also propose a solution to efficiently create secret on-chip. As a last contribution, we outline how to transform our idea into a circuit for true random number generation

REFERENCE

[1]. Kassabalidis I , El-Sharkaw M A,Marks R J.Swarm intelligence for routing in communication networks,Global Telecommunications, vol. 6,pp. 3613-3617,2001

[2]. Camilo T,et al.,An Energy-Efficient Ant-Based Routing Algorithm for Wireless Sensor Networks[C],Proceeding of ANTS 2006-the 5th Internationnal Workshop on Ant Colony Optimization and Swarm Intelligence, Brusels,Belgium, pp.49-59, 2006.

[3]. Jiao Bin, Xiong Youping. Application of improved ant colony optimization algorithm in wireless sensor networks,Journal of Jilin University, vol. 41,pp. 215-218, 2011.

[4]. Luo Xu, Wu Xiaojun. Application of ant colony optimization algorithm in WSN routing,computer engineering and science, vol. 37, pp. 740-746,2015.

[5]. S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," IEEE Trans. Dependable Secure Comput., vol. 5, no. 4, pp. 208–223, Oct.- Dec. 2008.

[6]. Y.-L. Huang, F.-Y. Leu, and K.-C. Wei, "A secure communication over wireless environments by using a data connection core," Math. Comput. Modelling, vol. 58, no. 5, pp. 1459–1474, 2013.

[7]. A. Castiglione, G. Cattaneo, A. De Santis, F. Petagna, and U. Ferraro Petrillo. 2006. "SPEECH: Secure personal end-to-end communication with handheld," in Proc. ISSE Securing Electronic Busines Processes. Vieweg, pp. 287–297, [Online]. Available: http://dx.doi.org/10.1007/978-3-8348-9195-2_31

[8]. Y.-L. Huang, F.-Y. Leu, I. You, Y.-K. Sun, and C.-C. Chu. (2014). A secure wireless communication system integrating RSA,

DiffieHellman PKDS, intelligent protection-key chains and a Data Connection Core in a 4G environment. J. Supercomput. [Online]. 67(3), pp. 635–652. Available: http://dx.doi.org/10.1007/s11227-013- 0958-z

[9]. James Henrydoss, Terry Boult Department of Computer Science, University of Colorado at Colorado Springs, Colorado Springs, CO. – 2014" Critical Security Review and Study of DDoS Attacks on LTE Mobile Network"978-1-4799-3711

[10]. R. Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions", IEEE.

[11]. M. Ma, "Security Investigation in 4G LTE Networks", IEEE GLOBECOM 2012. http://www.ieeeglobecom.org/2012/private/T10F.pdf

[12]. M. Abid, S. Song, H. Moustafa, and H. Afifi, " Efficient Identity-based Authentication for IMS Based Service Access", Proceedings of the 7thInternational Conference on Advances in Mobile Computing and Multimedia (MoMMM '09), 2009.

[13]. D. Jones, Mobile Editor, "2014: A VoLTE Security Nightmare?" http://www.lightreading.com/mobile/mobile-security/2014-a-volte-securitynightmare/