Prevention of Network Energy in Ad-Hoc WSN

Alamelu.V[1], S.Thilagamani[2]

[1]Assistant Professor, Department of CSE, M.Kumarasamy College of Engineering, Karur.

[2]Professor, Department of CSE, M.Kumarasamy College of Engineering, Karur. E-Mail: sthilagamani11@gmail.com

Abstract - In sensing and pervasive computing, low-power networks relate the moving analysis direction. At routing protocol layer, resource depletion attack is explored which leads to draining of battery power rapidly. The “vampire” attack is not specific to a protocol, even though it has similarities in characteristics with various standard routing protocols. Every protocol is subject to attacks. In worst case, one attack will enhance the energy usage of network by an element of O (N0, wherever N within variety of network nodes. Discussed the strategies to ease these methods of attacks, in addition to a substitute of proof-of-concept protocol that certainly limits the harm caused by Vampires all through the packet forwarding part.

Keyword - Wireless sensor Network, vampires, clustering algorithm, transmission

I. Introduction

A Wireless Sensor Network (WSN) is spotted to examine the physical and environmental situations and to transfer data through network. For military applications, the wireless sensor network growth was motivated. Now-a-days, such networks are widely used in industry, consumer applications, process monitoring, health monitoring and so on.

II. Literature review

A. Object Recognition Based on Image Segmentation and Clustering

Through two separate methods, former information of image is retrieved. First method includes detection of object parts in an image and followed by integration of detected parts into clusters. Visual words is formed by combining all cluster centers. The later method involves the super pixel segmentation from an image and using Mid-level clustering algorithm forms a larger sub-region. The result of both methods shows the similarity of object segmentation. In addition the matrix representation for the shape and color or texture has been used. The probability of each super pixel is ensured by Mask map.

B. Boundary Recognition In Sensor Networks By Topological Methods

Wireless sensor networks are strongly tied with geometric environment. Environment monitoring and data collection of sensor network application need adequate coverage region of interest. The global topology plays a vital role in basic design of network functionalities like data gathering and point-to-point routing methods. The boundaries contains physical correspondence like transportation of network, buildings, terrain variation, etc., Holes map with the events being monitored by sensor network. Consider the readings above the threshold as invalid, then hole boundaries form a iso-contours of landscape of the attribute. Holes are major indicators of inadequate coverage and connectivity. Physical destruction or power depletion are indicated by holes.

C. A High Throughput Path Metric for Multi-Hop Wireless Routing

Rapidly changing topology, scalability and coping with mobile nodes are the recent works in ad hoc routing. Lossy wireless links pay less attention in finding high-quality paths. It measures a link loss characteristics on 29-node 802.11 b test bed, and uses them in designing the new metric for lossy links. Minimum hop count is the common metric used in ad hoc routing protocol. These protocols uses the links that deliver routing probe packets. This method unconditionally assumes that either link works or not. Intermediate loss ratio is more in wireless links.

D. Denial of Service Resilience In Ad Hoc Networks

In securing ad hoc networks, significant progress has been made through the development of secure routing protocols. Significant research effort focuses on denial-of-service attack and ensuring flexibility. Flexibility is a difficult component of a secure system that seeks to reduce malicious nodes. Adversaries will continually increase the complicated attacks, so protocol developers will frequently design the protocol mechanism to prevent the fresh attacks. A goal is to calculate the victorious attacker can have on the concert of ad hoc network. The objective is to describe the association between the resources and the impact on non-attacking nodes presentation.

III. Existing System

Initially, Authorization process takes place by matching the login images of an authorized users [14][15]. Honest nodes transmit a message of original size to same destination using dissimilar packet headers. Vampire attack consumes more energy of nodes for transmission of message than the honest nodes. Malicious nodes energy usage is not considered because it drains its own battery power. Adversaries are malicious nodes has same resource and network level access as honest nodes. Adversary nodes are fixed and random within the network. Adversary nodes can destroy a number of honest nodes before the depletion of network. Intelligent adversary assignment or dynamic node compromise would cause more damage of the nodes. In constant charging case, battery power draining attack would be effective only if adversary is capable of consuming power as fast as honest nodes can revive. The disadvantages are power draining, Reduction of Quality (RoQ), and difficult to detect and prevent the vampire attack.

IV. Proposed System

Proposed a PLGP, a protocol to provide the backtracking details. A network with a group of nodes, connectivity properties, a topology and node identities are used. Honest nodes can do broadcasting and receiving communication. Malicious nodes use directional antennas to transfer the data without being overheard by another node. Honest node compose, forward and accept/drop messages. Malicious node randomly transfers the data. Adversary nodes cannot damage the connectivity between any two honest nodes because all messages are signed by the originator. Rather, adversary nodes can alter, shorten or remove the packet fields. The advantages are to evaluate the vulnerabilities of existing protocol battery depletion attack. It prevents the routing infrastructure. It protects the packets getting damage from vampire attack.

V. Conclusion

A latest resource utilization vampire attack that use routing protocol to eternally halt wireless sensor network by reducing nodes battery power. These attacks fairly expose the vulnerabilities in a number of protocol classes rather it don’t depend on particular protocol. On a arbitrarily generated topology of 50 nodes calculated a proof-of-concept attacks beside delegate examples of existing routing protocols using feeble adversaries. The network routing protocol PLGPa, limits the damage from vampire attack and verifies that packets always progress towards their destination.

References

[1] Aad.I, Hubaux.J.P, and Knightly.E.W, (2004) “Denial of Service Resilience in Ad Hoc Networks,” Proc. ACM MobiCom.

[2] Acs.G, Buttyan.L, and Vajda.I, (Nov.2006) “Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546.

[3] S.Thilagamani, N. Shanthi, “Object Recognition Based on Image Segmentation and Clustering”, Journal of Computer Science,Vol. 7,No.11,pp. 1741-1748, 2011.

[4] Aura.T, (2001) “Dos-Resistant Authentication with Client Puzzles,” Proc. Int’l Workshop Security Protocols.

[5] S.Thilagamani, N. Shanthi, “Gaussian and gabor filter approach for object segmentation”, Journal of Computing and Information Science in Engineering,Vol.14,Issue 2, pp. 021006,2014

[6] Bellardo.J and Savage.S, (2003) “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. 12th Conf. USENIX Security.

[7] Bernstein.D and Schwabe.P, (2008) “New AES Software Speed Records,” Proc. Ninth Int’l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT).

[8] Bernstein.D.J, (1996) “Syn Cookies,” http://cr.yp.to/syncookies.html.

[9] Blaked.I.F, Seroussi.G and Smart.N.P, (1999) Elliptic Curves in Cryptography, vol. 265. Cambridge University.

[10] Bos.J.W, Osvik.D.A and Stefan.D, (2009) “Fast Implementations of AES on Various Platforms,” Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org.

[11] Chan.H and Perrig.A, (Oct.2003) “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105.

[12] “The Network Simulator - ns-2,” http://www.isi.edu/nsnam/ns,2012.

[13] E.T. Venkatesh , P. Thangaraj , and S. Chitra , “ An Improved Neural Approach for Malignant and Normal Colon Tissue Classification from Oligonucleotide Arrays ,” European Journal of Scientific Research , vol. 54 , pp. 159 – 164 , 2011.

[14] S.Thilagamani,N. Shanthi, “Literature survey on enhancing cluster quality”, International Journal on Computer Science and Engineering Vol. 02, No. 06, pp1999-2002, 2010.

[15] V.Baby Deepa, P.Thangaraj, S.Chitra,” Investigating principal component analysis for classification of EEG data”, International Conference on Networking and Information Technology (ICNIT), PP.461-464, 2010.

[16] E.T.Venkatesh,P.Tangaraj, S. Chitra, “Classification of cancer gene expressions from micro-array analysis”, International Conference Innovative Computing Technologies (ICICT), 2010.