ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 3, March 2016

Review paper on Cost-aware secure routing protocol (CASER) in MANET with power optimization

Akanksha.G.Heda, Prof. Prajakta.P.Nalgirkar, Prof. Vidhya.H.Deshmukh

Abstract- **A novel secure and efficient Cost-Aware secure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic based random walking. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. For this propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. Here also provide a quantitative security analysis on the proposed routing protocol. The theoretical analysis and OPNET simulation results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, the analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. Thisdemonstrate that the proposed CASER protocol can achieve a high message delivery ratio while preventing routing trace back attacks**.

***Index items*:- CASER,WSN,OPNET**

I. INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties Routing is another very challenging design issue for WSNs. A properly designed routing protocol should notonly ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. Motivated by the fact that WSNs routing is often geography-based secure and efficient Cost-Aware secure routing (CASER) protocol for WSNs without relying on flooding. CASER allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework. The distribution of these two strategies is determined by the specific security requirements. This scenario is analogous to delivering US Mail through USPS: express mails cost more than regular mails; however, mails can be delivered faster. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. CASER protocol has two major advantages:

(i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.

(ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing trace back attacks and malicious traffic jamming attacks in WSNs

II. WORKING

A. Source-Location Privacy in Energy-Constrained Sensor Network Routing

Source-location privacy is critical to the successful deploymentof wireless sensor networks. In this paper wefirst propose and analyze a routing-based scheme throughsingle-intermediate node. Then two multi-intermediate node schemes are introduced. For each of these schemes, we carriedout simulations to evaluate the performances. Simulation resultsdemonstrate that the proposed schemes can achieve verygood performance in energyconsumption, message deliverylatency and message delivery ratio.

B. Security in Wireless Sensor Networks: Issues and Challenges

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy

nonrepudiation, and anti-playback The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increasedFor the secure transmission of various types of information over networks, several cryptographic, steganography and other techniques are used which are well known. Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms).

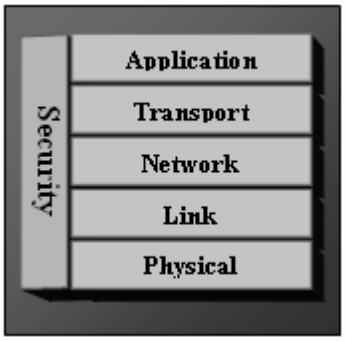

***Fig*:Holistic view of Security in wireless sensor networks**

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

C. Maximum Lifetime Routing In Wireless Sensor Networks

The problem of routing messages in a wireless sensor network so as to maximize network lifetime is NP-hard. In our model, the online model, each message has to be routed without knowledge of future route requests. Here develop also an online heuristic tomaximize network lifetime. Our heuristic, which performs two shortest path computations to route each message, is superior to previously published heuristics for lifetime maximization– our heuristic results in greater lifetime and its performance is less sensitive to the selection of heuristic parameters. Additionally, our heuristic is superior on the capacity metric.A new online heuristic– OML–for lifetime maximization. Extensive simulations show that new heuristic is superior to previously published heuristics for lifetime maximization both in terms of providing larger lifetime and in terms of sensitivity to algorithm parameters. Additionally, proposed heuristic provides larger network capacity than provided by competing heuristics

D. Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks

Source-location privacy is critical to the successful deployment of wireless sensor networks. In this paper, we first propose and analyze a routing-based scheme through single-intermediate node. Then two multi-intermediate nodes schemes are introduced. For each of these schemes, we carried out simulations to evaluate the performances. Simulation results demonstrate that the proposed schemes can achieve very good performance in energy consumption, message delivery latency and message delivery ratio.

E. Energy Aware Routing for Low Energy Ad Hoc Sensor Networks

These schemes typically try to find the minimum energy path to optimize energy usage at a node. In this we take the view that always using lowest energy paths may not be optimal from the point of view of network lifetime and long-term connectivity. To optimize these measures, a new scheme called energy aware routing that uses sub-optimal paths occasionally to provide substantial gainsa new routing protocol that is suitable for low energy and low bit rate networks. The idea behind the protocol is very simple – using the lowest energy path always is not necessarily best for the long-term health of the network.

Thus using a simple mechanism to send traffic though different routes helps in using the node resources more equitably. Using probabilistic forwarding to send traffic on different routes provides an easy way to use multiple paths without adding much complexity or state at a node. Network survivability is a very important criterion for deciding the efficacy of network protocols. It includes a measure of the network lifetime as well as the kind of service it provides during its life. Both these factors are important in evaluating networks and neither can be considered in isolation.

F. *Routing with Guaranteed Delivery in ad hoc Wireless Networks*

Mobile ad hoc networks (Manets) consist of wireless hosts that communicate with each other in theabsence of infrastructure. Two nodes in a manet can communicate if the distance between them is less than the minimum of their two broadcast ranges. Because stations whose broadcast areas overlap can interfere with each other and also because of health problems that can occur because of long-term exposure to powerful radio signals , it is generally not possible (or desirable) for all hosts in a manet to be able to communicate with each other directly. Thus, sending messages between two hosts in a Manet may require routing the message through intermediate hosts. In many cases, Manets are pieced together in an uncontrolled manner, changes in topology are frequent and unstructured, and hosts may not know the topology of the entire network. Consider routing in manets for which hosts know nothing about the network except their location and the locations of the hosts to which they can communicate directly. In particular, we consider the case in which all hosts have the same broadcast rangeAlgorithms for routing, broadcasting and geocasting in unit graphs. The algorithms do not require duplication of packets, or memory at the nodes of the graph, and yet guarantee that a packet is always delivered to (all of) its destination(s).

G. *GPSR: Greedy Perimeter Stateless Routing for Wireless Networks*

Information about a router's immediate neighbors in the Network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the *perimeter* of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly. We describe the GPSR protocol, and use extensive simulation of mobile wireless networks to compare its performance with that of Dynamic Source RoutingGPSR, a routing algorithm that uses geography to achieve small per-node routing state, small routing protocol message complexity, and extremely robust packet delivery on densely deployed wireless networks.

III. CONCLUSION

In this paper I have tried to cover both early and recent literature related to cost, security, power and packet delivery ratio which is all in one provided by CASER protocol algorithms and techniques. The aim was to introduce the current techniques. The evaluation of these techniques can be done, in terms of: performance to balancethe energy consumption and increase network lifetimeor We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime

IV. REFERENCES

[1] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[2] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[3] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. 6th Annu. Int. Conf. Mobile Comput.Netw. New York, NY, USA, 2000, pp. 243–254.

[4] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in Proc. 6th Annu. Int. Conf. Mobile Comput.Netw, 2000, pp. 120–130.

[5] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput.Netw., 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks," Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoo localization for very small devices," Comput. Sci. Dept., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729, Apr. 2000.

[8] A. Savvides, C.-C.Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu.Int. Conf. Mobile Comput.Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., 1999, pp. 48–55.

[10] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[11] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf.,Mar. 17–21, 2002, vol. 1, pp. 350–355.

[12] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 609–619, Aug. 2004.

[13] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

[14] F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2258–2267, Jul. 2010.

[15] C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F.Chou, and C.-J. Tu, "Onenhancing network-lifetime using opportunistic routing in wireless sensor networks," in Proc. 19th Int. Conf. Comput. Commun.Netw., Aug. 2010, pp. 1–6.

[16] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 88–93.

[17] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, Jun. 2009, pp. 493–501.

[18] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., Mar. 15–19, 2010. pp. 1–9.

[19] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008, pp. 51–55.

[20] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2005, pp. 599–608.

[21] Wikipedia. Quartic function [Online]. Available: http://en.wikipedia.org/wiki/Quartic_function, Apr. 2014.

[22] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," IEEE Netw., vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[23] A. Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: Issues and challenges," in Proc. 8th Int. Conf. Adv. Commun. Technol., 2006, pp. 1043–1048.