ISSN: 0976-3376

Available Online at http://www.journalajst.com

ASIAN JOURNAL OF
SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology
Vol.07, Issue, 03, pp.2653-2657, March, 2016

RESEARCH ARTICLE

REVIEW ON THE DETECTION OF SINKHOLE ATTACK IN WSN

*Rupali Prajapati and Rajni Dubey

Department of Computer Science, SRCEM, Banmor, Gwalior, India

ARTICLE INFO

Article History:
Received 19th December, 2015
Received in revised form
13th January, 2016
Accepted 21st February, 2016
Published online 31st March, 2016

Key words:

WSN,
Multipath,
Sinkhole.

ABSTRACT

Wireless Sensor network (WSN) is being emerged as a prevailing science in future as a result of its vast range of functions in military and civilian domains. These networks are simply prone to security attacks. Unattended set up of sensor nodes within the environment explanations many security threats in the WSNs. There are a lot of feasible attacks on sensor network. Sinkhole attack is likely a standout amongst the most destructive routing attacks for these networks. It ought to justification the interloper to bait all or loads of the data flow that must be caught on the base station. When sinkhole attack has been executed and the adversary node has begun to work as network member within the data routing, it may possibly practice some more threats corresponding to black gap or grey hole. Finally this drop of some predominant data packets can disrupt the sensor networks completely. We now have awarded some countermeasures in opposition to the sinkhole attack.

INTRODUCTION

WSNs have drawn reasonable quantity of research awareness in the course of last decade. Their restricted resources along with the antagonistic deployment environment put severe challenges to their search reports. More than a few aspects of such networks had been already studied and these forms of networks are actually well established for many functions starting from habitat monitoring to surveillance (Akyildiz *et al.,* 2002). Security is a crucial drawback in WSNs. Without availability, data confidentiality and integrity many real-world purposes of WSNs are in useless. Consequently, many reviews were excited by delivering security solutions for these networks (Perrig *et al.,* 2004). Detection and mitigation of attacks towards WSNs has been an appealing topic amongst researchers, above all, considering the fact that the distinctive challenges of those networks which might be normally imposed by using their useful resource constraints. Many varieties of attacks were offered, analyzed and eradicated in the literature (Perrig *et al.,* 2004; Chan, 2003). Sinkhole attack is one of the earliest among them that has been identified in WSNs (Karlof and Wagner, 2003). Sinkhole attack threatens the safety of WSNs at just about each layer of their protocol stack. The foremost deception of the attack is that a malicious node attracts the traffic of its neighbors by using pretending that it has the shortest direction to the bottom-station. The attack may just jeopardize many principal protection measures.

The sinkhole could launch a sort of attacks against the data traffic, comparable to selectively shedding the data packets, tampering data aggregation algorithms or interfering with clustering protocols. More than a few strategies had been proposed to combat the attack both through manipulation of routing algorithms (Villalpando *et al.,* 2008; Choi *et al.,* 2009) or by way of utilization of an IDS (Krontiris *et al.,* 2008; Krontiris *et al.,* 2008).

Multipath Routing in WSN

Multipath routing method is utilized as probably the most feasible resolution to cope with the obstacle of single-path routing strategy. This part grants the incentive in the back of utilizing multipath routing approach and in addition discusses the fundamental design issues within the development of multipath routing protocols. Data Reliability: Reliable data transmission in WSNs is a challenging task. Multipath routing technique presents resilience to node or link failure and trustworthy information transmission. There are two different strategies to furnish reliable data delivery by means of multipath routing. The first approach is finished via sending more than one copies of the identical data on a couple of paths to make sure packet recovery from course screw ups. A further process utilized by one of the existing protocols is erasure coding to furnish reliability. In this coding procedure, each supply node adds some additional expertise to the usual data packets after which distributes generated information packets over distinctive paths. For that reason, in order to reconstruct the long-established packets, a certain number of data packets from every source node must be got by means of the sink

Corresponding author: Rupali Prajapati
Department of Computer Science, SRCEM, Banmor, Gwalior, India

node. Despite the fact that the delivery of some data packets to the sink node fails, nonetheless ensures reliability with the aid of reconstructing data packets from effectively obtained data packets by means of the sink node. Multi path routing in WSN plays an important role in improving Fault Tolerance, Load Balancing (He *et al.,* 2008; Wang *et al.,* 2007), Bandwidth Aggregation (Tsai and Moors), QoS Improvement (Lou *et al.,* 2006; Tarique *et al.,* 2009). Every multipath routing protocol entails several accessories to construct more than one paths and distribute site visitors over discovered paths. These components are described beneath. Path Discovery: As the info transmission in WSNs is typically performed through multi-hop knowledge forwarding methods, the main purpose of route discovery procedure is to verify a collection of intermediate nodes that will have to be selected to be able to assemble several paths from source to sink nodes. One of a kind parameters are used to make routing choices and amongst these the most important parameter which is utilized is the amount of course disjointedness to detect several paths from each and every sensor node to the sink node (Lou *et al.,* 2006; Wegmulle *et al.,* 2000).

Node-Disjoint Multipath

Refers to set of paths wherein there is not any common node among the found out paths. Hence, they are unaffected by means of node failure on the other paths. Node-disjointedness provides better aggregated community resources. However because of random deployment of sensor nodes, it's elaborate to seek out large set of node-disjoint paths between sensor nodes and sink nodes.

Link-Disjoint Multipath

Refers to set of paths wherein there is no shared link between the paths but may share some customary intermediate nodes. Node failure in a collection of hyperlink-disjoint paths may just impact several paths that shared the failed node.

Partially-Disjoint Multipath

Refers to set of paths which can share a number of links or nodes between unique paths. Any link or node failure in a collection of in part-disjoint paths could deactivate a number of paths. Still establishing multiple partially disjoint paths can be with ease performed.

Path Selection and Traffic Distribution

After discovering a couple of paths, yet another predicament that needs to be addressed is the number of paths that will have to be chosen for data transmission. Thus, as a way to meet the performance demands of the meant software, proposing a route decision mechanism to pick a distinctive number of paths is an principal a part of designing high-performance multipath routing protocol. After choice of set of paths among the many discovered paths, multipath routing protocol will have to now verify the way to distribute the traffic over selected paths. Quite a lot of traffic allocation mechanisms are utilized to distribute the data amongst the selected paths.

Path Maintenance

In multipath routing, utilization of multiple paths from supply nodes to the sink nodes wants to be maintained periodically in an effort to acquire riskless data supply. If the path is damaged, then the sensor nodes ought to prefer a further most fulfilling route. For this reason route reconstruction must be supplied to lessen performance degradation. Route rediscovery process is initiated in three distinctive circumstances:

- When an active path fails
- When a certain number of active paths have failed
- When all the active paths have failed

Performing a route discovery process after the failure of an active node imposes high overhead. Initiating a route discovery process after the failure of all the active paths significantly reduces the network performance. Thus initiating a route discovery process after a certain number of active paths have failed may present a trade-off between the advantage and disadvantage of the first two approaches.

Sinkhole Attack in WSN

In a sinkhole attack, the adversary's purpose is to trap nearly all the site visitors from a designated subject by method for a compromised node, making an allegorical sinkhole with the enemy on the inside. Sinkhole attacks likely work by means of making a compromised node appears peculiarly alluring to surrounding nodes as for the routing algorithm. Sinkhole attacks are problematic to counter considering the fact that routing understanding furnished via a node is complex to affirm. As an illustration, a desktop-classification adversary has a powerful power radio transmitter that makes it possible for it to furnish an excessive-high-value route by means of transmitting with enough vigor to reach a broad discipline of the network. As shown in fig.1 a compromised node attracts the entire traffic from its neighbours via telling its neighbour that it has shortest route to arrive to the bottom station. This route is artificial high value route (Vinay Soni *et al.,* 2013). Fig. 3 denotes how sinkhole is created using wormhole. As shown in figure, one malicious node attracts all the traffic and make a tunnel with another malicious node to reach to the base station.

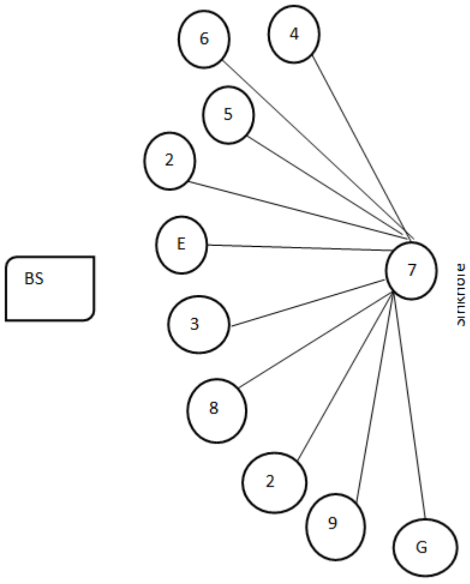

Fig.1. Demonstration of a sinkhole attack

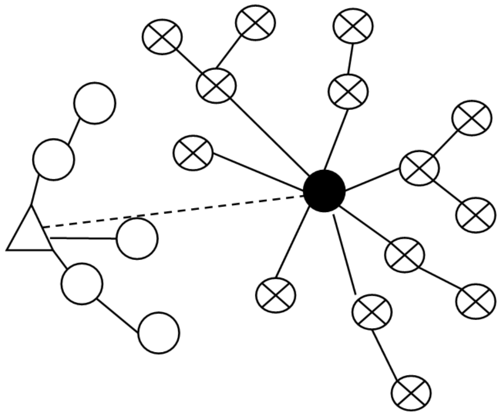

Fig. 2. Sinkhole using an artificial high quality route

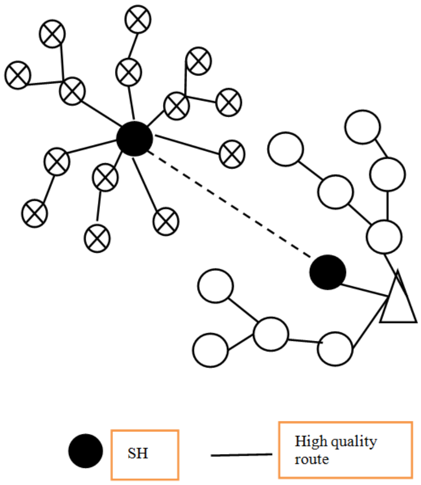

Fig. 3. Sinkhole using a wormhole

Sinkhole attack is one of the ruthless attacks in wireless Ad hoc network. In sinkhole Attack, affected node or suspicious node broadcast erroneous routing information to generate itself as a particular node and obtains entire network data. After receiving entire network information it alters the confidential information, such as changes made to data packet or drops them to make the network complicated. A suspicious node attempts to attract the secure data from all neighboring nodes (Ahmad Salehi *et al.,* 2013). The sinkhole attack is a in general strict attack that avoids the bottom station from attaining full and correct gazing data, hence making a severe threat to larger-layer applications. In a Sinkhole attack a affected node attempts to attract the whole community traffic as probable from a precise area, by way of forming itself to be noticeable as appealing to the adjoining nodes with appreciate to the routing metric. As a end result, the opponent manages to attract the complete visitors that's routed to the base station. By way of taking part in the routing procedure, then initiate more rigorous attacks. A compromised node does not always ought to goal different nodes from areas external its local in an effort to manage network traffic. The adversary needs handiest to launch the sinkhole attack from a node as close as feasible to the bottom station. In this case, by having the neighboring nodes decide upon the intruder as their guardian, all of the visitors coming from their descendants may also come to be within the sinkhole. So the attack can be very potent even if it's launched in the neighborhood, with small effort from the aspect of the attacker (Ahmad Salehi *et al.,* 2013).

Preventive approaches against Sinkhole Attack

Data Consistency and Network Flow Information Approach

The strategy offered in (Edith, 2006) involves the bottom station within the detection process, resulting in a high verbal exchange rate for the protocol. The base station floods the network with a solicitation message containing the IDs of the affected nodes. The influenced nodes answer to the base station with a message containing their IDs, id of the following hop and the related fee. The acquired understanding is then used from the bottom station to construct a community flow graph for picking out the sinkhole. The algorithm is also amazing to take care of cooperative malicious nodes that attempt to conceal the actual intruder. The efficiency of the proposed algorithm has been examined via both numerical evaluation and simulations. The results have validated the effectiveness and accuracy of the algorithm. They also endorse that its verbal exchange and computation overheads are reasonably low for WSNs.

Hop Count Monitoring Scheme

A novel intrusion detection system that detects the presence of a sinkhole attack is proposed in (Daniel Dallas *et al.,* 2007). The scheme is founded on hop rely monitoring. Considering the hop-count feature is effortlessly obtained from routing tables, the advertisements (Anomaly Detection process) is simple to enforce with a small footprint. Furthermore, the proposed advertisement is relevant to any routing protocol that dynamically keeps a hop-count parameter as a measure of distance between supply and destination nodes. The scheme can notice attacks with ninety six% accuracy and no false alarms making use of a single detection system in a simulated network.

RSSI Based Scheme

A new approach of robust and lightweight solution for detecting the sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages is proposed in (Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, 2009). The proposed arrangement needs coordinated effort of some Extra Monitor (EM) nodes separated from the ordinary nodes It utilizes estimations of RSSI from four EM nodes to decide the position of all sensor nodes where the Base Station (BS) is situated at origin position (0, 0). This data is utilized as weight from the BS keeping in mind the end goal to distinguish Sinkhole attack. The reproduction results demonstrate that the proposed mechanisms lightweight because of the monitor nodes were not stacked with any ordinary nodes or BS. The proposed mechanism does not bring about the correspondence overhead.

Monitoring node's CPU usage

A novel algorithm for detecting sinkhole attacks for substantial scale WSNs is examined in (Changlong Chen *et al.,* 2010). The detection issue is figured as a change-point detection issue. The CPU utilization of every sensor node is checked and analyzes the consistency of the CPU use. By monitoring the CPU use of every node in settled time interim, the base station calculates the difference of CPU utilization of every node. In the wake of contrasting the difference and a limit, the base station would distinguish whether a node is malicious or not. In this manner, the proposed algorithm can separate between the malicious and the legitimate nodes.

Mobile Agent Based Approach

The scheme to defend against sinkhole attacks using mobile agents is proposed in (Sheela *et al.,* 2011). Mobile agent is a application section which is self controlling. They navigate from node to node no node not only transmitting data but in addition doing computation. A routing algorithm with more than one constraints is proposed centered on mobile agents. It makes use of mobile agents to acquire knowledge of all mobile sensor nodes to make every node mindful of the complete community so that a valid node won't listen the cheating knowledge from malicious or compromised node which leads to sinkhole assault. It does now not need any encryption or decryption mechanism to become aware of the sinkhole attack. This mechanism does now not require extra vigour than common routing protocols.

Using Message Digest Algorithm

Detection of sinkhole attack in WSNs utilising message digest algorithms is proposed in (Sharmila and Umamaheswar, 2011). The principal purpose of the protocol is to observe the designated sink hole utilizing the one-manner hash chains. In the proposed process vacation spot detects the attack handiest when the digest received from the trustable ahead direction and the digest bought by means of the trustable node to the vacation spot are distinctive. It additionally ensures the data integrity of the messages transferred utilising the trustable course. The algorithm is also robust to handle cooperative malicious nodes that attempt to cover the actual intruder. The functionality of the proposed algorithm is tested in MAT lab.

Literature Survey

(Samundiswary and Dananjayan *et al.,* 2010)a secured route redundancy algorithm has been utilized to implement in heterogeneous sensor networks through incorporating alternate path scheme in these networks with mobile nodes for mobile sinks to look after towards sinkhole attacks. They used a heterogeneous sensor network model consisting of a few powerful high-end sensors and a large number of low-end sensors. They expanded path redundancy-based security algorithm for heterogeneous sensor networks by incorporating alternate path mechanism and mobility model for nodes and sinks to secure the nodes from sinkhole attacks in HSN. The proposed method is not suitable for homogenous sensor networks. Bahekmat *et al*., (2012) the devised algorithm, at the point when a node needs to forward data to the base station, firstly forwards a control packet straightforwardly to the main base station. After that it starts forwarding data packets to the base station in form of hop by hop routing. When the data packet is reached at the base station, some of its control fields are distinguished with the similar ones of the original control packet. If any modifications have been done to these control fields of the data packet, it demonstrates that there is a suspicious node; the base station identifies it by employing the devised scheme. At the start, the base station forwards its position to every node. The devised work is suitable for event driven applications. Whenever node detects an event, a control packet is sent to the BS using single hop communication. The control packet contains the following information: the unique number of the control packet (id), the transmitter node (Nid), data packet identifier (Pid) and the size of the data packet (Psize). After direct transmission of this packet to the BS, the transmitter node, depending on its routing table, sends data packet to its next hop node. The data packet is routed hop by hop until it receives to the BS. After comprehending the presence of a suspicious node in network, base station verifies data transmission route and stores currents nodes in its memory. Once base station identifies the presence of flaws in a packet constantly, it verifies the route every time and compares the nodes stored in memory with the fresh route, keeping comparable nodes in memory and removing the remaining data. As per, base station identifies the suspicious node, notifying other nodes not to send data to suspicious node further more. Manisha *et al.,* (2013) present that WSN platforms are less costly and more influential incorporating small electronic devices named as Motes. WSNs improve its reputation in defense and health centric research region; as well as accepted in industrial region. Author presents the security perquisites as WSNs are simply vulnerable to more attacks than wired networks.

Rajkumar *et al.,* (2013), in respect to give whole resolution to identify and avoid sinkhole attack a Leader Based Intrusion Detection System is devised. In this approach a leader is chosen for every group nodes within the network, region wise and it equates and estimates the nature of each node sensibly performs detection module and observes every node nature among the group for any sinkhole attack to take place. When a node gets recognized as a affected node, it notify that nodes status to the other leader within the WSN, such that every leaders present in the network are aware of the sink hole node and the leaders discontinue transmission with sinkhole node. In this technique they enhanced the performance of the system by means of energy efficiency and intrusion detection rate. Zhang *et al.,* (2014), The most important contribution is to endorse a brand new Sinkhole detection algorithm focused the multi-way selection. The reproduction likewise demonstrates the feasibility of the technique. As a way to restrict sinkhole assault, we do some research on it, and one approach to watch the sinkhole attack, jogged on the redundancy mechanism is proposed on this paper. For the suspicious nodes, messages are despatched to them through multi-paths. With the aid of evaluating the answered comprehensively, the attacked nodes are eventually confirmed.

Conclusion

With the advances in science, there was an growing curiosity in the usage of WSNs. Protection is a imperative challenge in WSNs. Without availability, data confidentiality and integrity many actual-world applications of WSNs are in vain. WSNs are prone to a huge type of attacks among which sinkhole attack places extreme threats to the security of such networks. On this study, we have surveyed various countermeasure techniques for sinkhole attack.

REFERENCES

Ahmad Salehi, S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala;" Detection of Sinkhole Attack in Wireless Sensor Networks". Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013

Akyildiz, I., W. Su, Y. Sankarasubramaniam, E.Cayirci, Wireless sensor networks: asurvey, Computer Networks 38(4)(2002) 393–422.

Chan, H., A. Perrig, Security and privacy in sensor networks, Computer 36(10) (2003) 103–105.

Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth; "Detecting Sinkhole Attacks in Wireless Sensor Networks" ICROS-SICE International Joint Conference 2009, pp. 1966-1971.

Changlong Chen, Min Song, and George Hsieh; "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks" *IEEE International Conference on Wireless Communications*, Networking and Information Security (WCNIS), 2010, pp. 711-716.

Choi, B., E. Cho, Kim, C. Hong, J. Kim, A sinkhole attack detection mechanism for LQI based meshrouting in WSN, in: Proceedings of International Conference on Information Networking, 2009, pp.1–5.

Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" 15th IEEE International Conference on Networks, 2007, ICON 2007, pp.176-181.

Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" *IEEE International Conference on Communications*, 2006, Volume 8, pp. 3383-3389.

Fang-Jiao Zhang, Li-Dong Zhai , Jin-Cui Yang , Xiang Cui; "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks*". Information Technology and Quantitative Management* (ITQM 2014)

He, T., Ren, F., Lin, C., Das, S. Alleviating Congestion Using Traffic-Aware Dynamic Routing in Wireless Sensor Networks. In Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08), San Francisco, CA, USA, 16–20 June 2008; pp. 233–241.

Karlof, C., D. Wagner, Securer outing in wireless sensor networks: Attacks and counter measures, AdHoc Networks 1(2) (2003) 293–315.

Krontiris, I., T. Dimitriou, T. Giannetsos, M. Mpasoukos, Intrusion detection of sinkhole attacks in wireless sensor networks , in : Algorithmic Aspects of Wireless Sensor Networks, 2008

Krontiris, I., T. Giannetsos, T. Dimitriou, Launching a sinkhole attack in wireless sensor networks; the intruder side, in : Proceedings of IEEE International Conference on Wireless and Mobile Computing, 2008, pp.526–531.

Lou, W., Liu, W., Zhang, Y. Performance Optimization Using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks. Combinator. Optim. Commun. Netw. 2006, 2, 117–146.

Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, and Sanaz Sadeghi;" A Novel Algorithm for Detecting Sinkhole Attacks in WSNs".*International Journal of Computer Theory and Engineering*, Vol. 4, No. 3, June 2012

Manisha, Gaurav Gupta," Attacks on Wireless Sensor Networks: A Survey",*International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 10, October 2013, Page 190- 197

Perrig, A., J. Stankovic, D.Wagner, Security in wireless sensor networks, Communications of the ACM 47(6)(2004) 53–57.

Samundiswary, P., PP, Dananjayan P. Detection of sinkhole attacks for mobile nodes in heterogeneous sensor networks with mobile sinks. *International Journal of Computer and Electrical Engineering* 2010;2:127e33.

Sharmila, S. and Dr G Umamaheswari; "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms" International Conference on Process Automation, *Control and Computing* (PACC) 2011, pp. 1-6

Sheela, D., Naveen kumar. C and Dr. G.Mahadevan; "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" *IEEE-International Conference on Recent Trends in Information Technology*, ICRTIT 2011, pp. 527-532

Tarique, M., Tepe, K.E., Adibi, S., Erfani, S. Survey of Multipath Routing Protocols for Mobile Ad Hoc Networks. *J. Netw. Comput. Appl.* 2009, 32, 1125–1143.

Tsai, J. and T. Moors, "A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks".

Udaya Suriya Rajkumar, D. and Rajamani Vayanaperumal;" A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network". *International Journal of Computer Science,* 2013

Villalpando, R., C.Vargas, D.Munoz, Network coding for detection and defense of sinkholes in wireless reconfigurable networks, in: Proceedings of International Conferenceon Systems and Networks Communications, 2008, pp.286–291.

Vinay Soni, Pratik Modi, Vishvash Chaudhri; "Detecting Sinkhole Attack in Wireless Sensor Network". *International Journal of Application or Innovation in Engineering and Management*, 2013.

Wang, C., Li, B., Sohraby, K., Daneshmand, M., Hu, Y. Upstream Congestion Control in Wireless Sensor Networks Through Cross-Layer Optimization. *IEEE J.* Select. Areas Commun. 2007, 25, 786–795.

Wegmuller, M., J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, pp. 109.

****