Energy Efficient Topology Maintenance using Adaptive Hello Messages in PLGPa

[1]N Jagadeesh
PG Scholar,
Department of Computer Science and Engineering,
University College of Engineering (BIT Campus),
Anna University Chennai,
Tiruchirappalli - 620024.
neuralblue@yahoo.co.uk

***Abstract*— Adhoc wireless sensor networks are limited resource constrained network. They are vulnerable to the many active adversaries due to its open and hostile environment. Active adversary within the network degrades the performance of the network by means of resource depletion; disturb routing, reliability of data transfer, wastage of CPU time and bandwidth consumption. PLGPa is a secure protocol to resist the various active adversaries within the network but less efficient in topology maintenance. In the most of the protocol link maintenance or topology maintenance are handled through periodic hello messages. But periodically sending hello messages to the nodes not in use or long term idle neighbor nodes are the energy draining and at the same time periodically sending hello message to the frequently communicating nodes are important. So, we proposed an adaptive hello messages which keeps the period of broadcasting hello message is depend on average event interval time. The modification in the discovery phase can make the topology maintenance efficient in PLGPa.**

Keywords—Topology Maintanance, Adaptive Hello messages, PLGPa, PLGPa-AH, Energy Efficient

I. INTRODUCTION

Adhoc wireless sensor network are limited with the resources like power, CPU Speed, Memory and Network Bandwidth. They are infrastructure less, self organizing networks for their operations. Due to this factor adhoc wireless sensor network relay on the cooperative routing process. In the any communication, sender is the primary node sends the packet and receiver alias sink is the one who receives the packet. In the adhoc, packet transmission between the source and sink is a cooperative process. The nodes between the source and sink will involve in the communication to transfer the packet to the sink. So all the node in the network will perform its primary function and act as routers to route the packet. Due to this a routing protocol design has various challenges. Very important and primary challenge is efficient in routing the packet and secure routing against the attack. Hidden perceptions of all the protocols are Reliable data transfer and energy efficient routing. As these networks are limited resources it's very important to be an energy efficient operation. Especially this PLGPa is designed to perform reliable data transfer between two nodes even in the active adversaries. Generally three mechanisms to design secure routing protocol are: prevention, detection/recovery, resilience. Prevention mechanism is well suits to the known attacks. Prevention mechanism restricts the attacks in the network. Malicious action in the network is restricted by the cryptographic techniques in the prevention mechanism. Prevention mechanisms are highly effective approach to find the well known attacks in the network. Detection/recovery approach is performed by monitoring the behaviors of the node involved in the network operations and other communication. If any malicious activity is identified in the monitoring process by detection mechanism, will call the recovery mechanism for the elimination of malicious node which performs the malicious action in the network. This detection and recovery mechanism are very helpful in the situation when the attacks are unknown. A resilience mechanism maintains the certain level of availability even in the adversarial environment. This protocol PLGPa incorporates all the three mechanism- prevention, detection/recovery and resilience for the secure routing and communication primitives. But there is very less efficient work in the topology maintenance of PLGPa.

Designing the energy efficient topology maintenance for PLGPa is quite difficult due to its organization in topology discovery. Main aim of the topology maintenance is to identify the broken links and new nodes in the network. Making this process as energy efficient is the quite challenging and essential work. Topology maintenance indirectly extends the connectivity life time of the network. At the same time make it as an energy draining process will decrease the life time of the network. For the well understanding we would like to define the term Topology control. Topology control consists of two operations one Topology construction and Topology Maintenance. As an initial and first step of network formation network will constructs topology by the node discovering in the network. Once the nodes in the network are discovered to its neighbor or other nodes in the network as protocol suggested. Once the protocol constructed for the initial stage it should be maintained till the life time of the network for purpose of packet forwarding within the network.

This paper proposes the energy efficient topology maintenance using the adaptive hello messages with event interval. They are dynamic to set the hello message interval time according to the amount of communication event in the network. Topology maintenance is hidden energy draining process in the infrequent communication networks. So suppression of the unwanted hello messages will reduce the energy consumption and also dynamic to set the interval is major advantage of the scheme that will suit for frequent and infrequent event based network to improve energy efficiency. In addition to that, paper discuses the Overview of PLGPa which is an extended version of PLGP. The various function performed by the PLGPa in the Topology discovery is also discussed.

II. PLGPa Overview

Secure sensor network routing: A clean – slate approach is modified in forwarding phase to avoid the damages caused by the vampire attacks are known as PLGPa. PLGPa is one of the secure protocols for avoiding various types of routing attacks through incorporating mechanism of Prevention, detection/recovery and resilience. PLGP consist of two phases one is discovery phase and forwarding phase. In discovery phase PLGP constructs network address by making all the nodes under one group using group merge algorithm. This discovered topology is shared by all the nodes and further packet transfer to sink will be done through the network address. Packet forwarding is individually decided by the node.

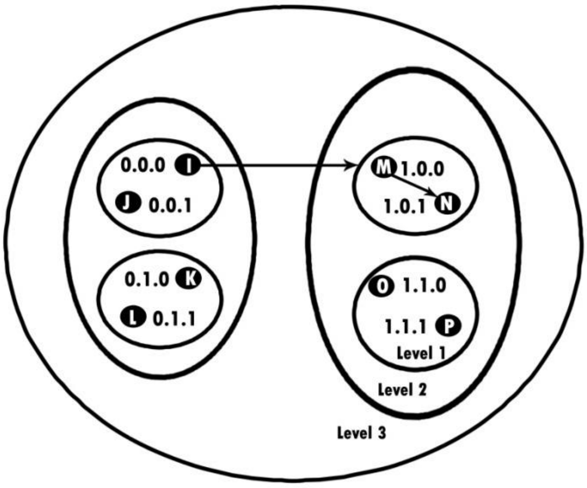

Fig 1. Recursive Grouping

Getting little bit deeper discussion the above diagram shows the simple illustration of recursive grouping in the topology discovery phase. Initially every node assumes itself a group with the size of one with its network address as zero. Then these groups with the size one will make the group merge proposal to other group in the network. As a next step, group will decide to merge with each other and forms the group size as two which is show in the figure as level1 where one node takes the value 0 as address and other takes 1 as a address. After that, again group will make a merge proposal to other group now network address for one group is prefixed with one and other with zero (refer level2). Generally this protocol suggests to merge group when there is group size is same and all the group members should agree for the merge. The process of merging groups will be proceed till the all the nodes comes under the single group. For the every merge function network address bit is increased to one.

Finally all the nodes in the network will come under one group and network address tree also constructed as shown in the figure. This topology network address tree is shared among all the nodes. So that, all the node will have the entire network topology knowledge which helps for the packet forwarding.

Following is the routing table of the node I where node I uses the table to decide the packet forwarding path. For example when node i want to transfer the packet to destination node N where source node network address is node I (0.0.0) to destination node N network address (1.0.1). Every node that forwards the packet should match its own address and destination address from the MSB. When it finds the difference at the particular bit it will forward towards that level region. Here destination address and source address different in the first bit so destination address mention it as 1 so according to the routing table of node I prefix with the 1 is the node M. so node I decides to forward the packet to node M. then node M matches with its address from the MSB 1.0 will match the difference will be the last bit which 1. Node M refers the routing table and will forward to the node N which is the destination.

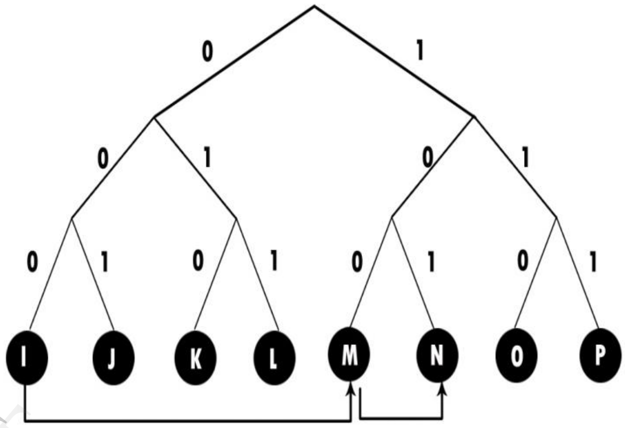

Fig 2. Network Address

Prefix	Next hop
1.*	M(1.0.0)
0.1.*	K(0.1.0)
0.0.1	J(0.0.1)

Table .1 Routing Table of node i

So, for the packet forwarding between the node I (source) to node N (destination) is moved through the path I->M->N with help of the network address. There is the chance one malicious node can claim group merge with many groups and member of many groups. Generally this is said to be a cloning. After the construction of network address, all the nodes will exchange the pair of information node id and network address with its neighbor. Replication detection algorithms are used to identify cloning node which may do malicious activity if clones are indentified in the network. PLGPa is the one of the secure routing protocols. Especially it is so secure and efficient in routing in ad hoc wireless sensor network. And also it consists of prevention detection/recovery and resilience mechanism for efficient secure routing functions and malicious node identification. But PLGPa is less efficient in the topology maintenance. PLGPa is modified as PLGPa-AH to support the Adaptive hello messages in PLGPa to improve the energy efficiency factor in topology maintenance. By making the topology maintenance energy efficient we can improves the life time of the network. As adhoc is resource constrained network, the efficient maintenance of network topology lets to the indirect benefits in energy consumption, bandwidth utilization, reliability of data transfer and other network operations.

III. Adaptive Hello Messages In PLGPa

Mentionable and conventional scheme used are periodic hello packet messaging. Considering this scheme, Td is the time for link failure detection, Tw is the time interval between the time Td and Tf which is represented as a time when node required for the forwarding. The time between the Td and Tf is Tw, where superfluous of multiple hello packets will be sent to detect the link failure. But it is only required at the time of Tf for the packet forwarding. This superfluous of multiple hello packets is the energy draining to the limited resources network. This scenario can be handled with the correction in the hello interval. Now let us consider the sender and neighbor who involves in the event of packet forwarding. Where neighbor moves out of the range of the sender. In this scenario two possible cases 1) sender requested to forward or 2) sender not required forwarding. For the case (1) link failure will occur, in case (2) it is not required to update link state of the neighbor. To prevent the link failure, sender should have the knowledge about the link. This knowledge can be obtained from the last received hello packet. If the hello packet is not valid to the time of the event then there is chance of sending packet through the unavailable link. So considering event interval to fix hello interval is important factor.

We propose a PLGPa-AH for energy efficient reliable data transfer in adhoc wireless sensor network. As adhoc is the limited resource network, energy is resource to be considered for less consumption. To maintain topology of the network, many protocols follow the hello message scheme to discover, maintain the topology and broken links. This hello message is the hidden draining energy in the situation like when the neighbors are rarely communication. Any node in the path may be a death node that affects route maintenance and throughput of the network. It is very important in the adhoc network to discover the neighbor for routing. Hello messages or beacon messages are used to discover the live neighbor. Various kind of these schemes are mentioned in literature [6] with no start time and end time which may cause the wastage to the energy and bandwidth. There are two approaches mention for reducing the hello messages packets [9] in the network. First we discuss here is on demand mechanism. In this mechanism hello packets are sent only at the time of the routing request and route reply, when there is on demand for the communication hello packets are sent. This will increase the delay in the packet transmission due to on demand hello messages. Second is event based hello packets will broadcast the hello messages to the any active nodes those who are sending or receiving the message based on threshold. Thresholds are mentioned activity timer. When the threshold communication is high then it is overhead and when threshold communication is low that's lets to local link information loss. Our proposed scheme dynamically adjusts the hello intervals for the hello packet broadcast. Consider that if the neighbor node never involved in any communication in the network for a period of time are not require to maintain the states of tits link and also hello packet to this node unwanted and energy draining. In our proposed scheme for PLGPa we took the event interval as a parameter set the hello message interval. Event interval is nothing but the time interval between two successive communications. Here communication can be mentioned to be a sending or receiving data packets. The proposed scheme saves energy and bandwidth of the network by suppressing the hello messages. Our proposed system is very dynamic to fix the interval according to the event interval. As the event interval increases hello message broadcast also increases and if it decreases then the broadcast also decreases. By using the adaptive hello messages throughput and reliability of the network can be increased with energy efficient topology maintenance.

Node death:

In the adhoc wireless sensor network some nodes will go to the death state due to the low battery power. As adhoc wireless sensor network is cooperative routing process, node routing table should aware of the death node for the reliable and effective routing in the network. Once if any node finds the broken link then, check for the companion or alternate path for the routing. In other words it can be mentioned as multipath forwarding.

Node Addition:

There are some needs of the application to add the nodes after the deployment of the network. In the PLGPa-AH whenever it finds the changes in the topology like addition of node, the protocol should rerun the grouping algorithm. In the protocol recursive grouping algorithm has two benefits one is to give the network address in the network topology tree and another to systematically eliminate death nodes from the network.

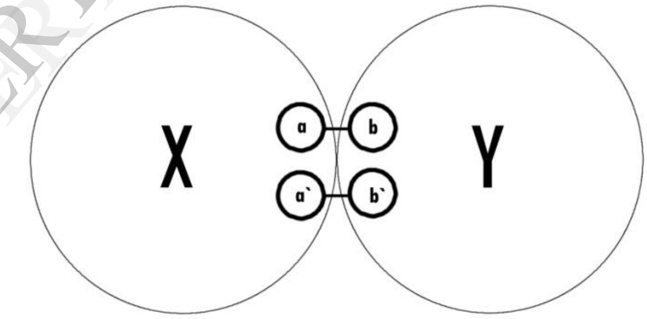

Fig 3. Merging Group

The figure shows the two groups X and Y. in those groups a, a', b and b' are the edge nodes for the group X and Y. if a and a' decide to merge with group Y then node a and a' will propagate the decision to the other nodes in the group. This will be done with a single broadcast within X.

Exchanging Merge Proposal:

Once all the node in the group agrees to merge with other group. Edge node take a responsibility of sending merge proposal to the neighbor group by means of edge node of the other group. If the other group refuse to merge for the merge proposal than the refuse merge will propagate through the edge nodes of the group.

Merging:

If group G and G' agrees to merge then it will form the new group GG' with the new group ID. All the nodes in the group will update the new neighbor, new topology and routing table entries.

Post Merge:

After the merge process, again the group will look for the merge proposal with the other group. This process will be continued till the all the group comes merged into a single group. PLGPa-AH is clever against the adversary in every merge proposal it prevents adversary with intention to modify or inject the false information through the verification of GVT. So, malicious node can only drop the merge proposal or not initiates the merge proposal will not be the performance degradation to the densely deployed adhoc wireless sensor network.

IV. CONCLUSION

This paper proposes the PLGPa-AH which is the PLGPa – adaptive Hello messages protocol. PLGPa is modified to adopt the adaptive hello message for the energy efficient topology maintenance. These adaptive hello message intervals are dynamic according to the event interval. If the event interval is more, then the hello message interval also more. The scheme suppresses the hello message for the less communication network so that energy efficiency can be increased. At the same time proposed scheme efficiently detects the broken links for the higher communication network.

REFERENCES

[1]. B. Parno, M. Luk, E. Gaustad, and A. Perrig, “Secure Sensor Network Routing: A Clean-Slate Approach,” CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[2]. Eugene Y. Vasserman and Nicholas Hopper “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

[3]. Seon Yeong Han and Dongman Lee “An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols", IEEE COMMUNICATIONS LETTERS, VOL. 17, NO. 5, MAY 2013.

[4]. Giruka and M. Singhal, “Hello protocols for ad-hoc networks: overhead and accuracy tradeoffs,” in Proc. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, pp. 354–361.

[5]. C.-M. Chao, J.-P. Sheu, and I.-C. Chou, “An adaptive quorum-based energy conserving protocol for IEEE 802.11 ad hoc networks,” IEEE Trans. Mobile Computing, vol. 5, no. 5, pp. 560–570, May 2006.

[6]. E. Belding-Royer and S. D. C. Perkins, “Ad hoc on-demand distance vector (AODV) routing,” July 2003..

[7]. C. Gomez, M. Catalan, X. Mantecon, J. Paradells, and A. Calveras, “Evaluating performance of real ad-hoc networks using AODV with hello message mechanism for maintaining local connectivity,” in Proc. 2005 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 2, pp. 1327–1331.

[8]. G. Iannello, F. Palmieri, A. Pescape, and P. S. Rossi, “End-to-end packet channel Bayesian model applied to heterogeneous wireless networks,” in Proc. 2005 IEEE Global Telecommunications Conference, pp. 484–489.

[9]. A.J. Goldsmith and S.B. Wicker, “Design Challenges for Energy-Constrained Ad Hoc Wireless Networks,” IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.

[10]. J. Hui and M. Devetsikiotis, “The use of metamodeling for VoIP over Wi-Fi capacity evaluation,” IEEE Trans. Wireless Commun., vol. 7, no. 1, pp. 1–5, Jan. 2008.

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

[12]. J. Hui and M. Devetsikiotis, “The use of meta modeling for VoIP over Wi-Fi capacity evaluation,” IEEE Trans. Wireless Commun., vol. 7, no. 1, pp. 1–5, Jan. 2008.

[13]. R. Oliveira, M. Luis, L. Bernardo, R. Dinis, and P. Pinto, “The impact of node’s mobility on link-detection based on routing hello messages,” in Proc. 2010 IEEE Wireless Communications and Networking Conference, pp. 1–6.

[14]. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless micro sensor networks. In Hawaii Int’l Conference on Systems Sciences, 2000.

[15]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly resilient, energy-efficient multipath routing in wireless sensor networks. Mobile Computing and Communication Review, 5(4):10–24, 2002.

[16]. T. Clausen, C. Dearlove, and J. Dean, “Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP),” 2010.