Adaptive Algorithms to Enhance Routing and Security for Wireless PAN Mesh Networks

Cao Trong Hieu[1], Tran Thanh Dai[1], Choong Seon Hong[2], and Jae-Jo Lee[3,*]

[1] Department of Computer Engineering, Kyung Hee University
Giheung, Yongin, Gyeonggi, 449-701 Korea
{hieuct, daitt}@networking.khu.ac.kr
http://networking.khu.ac.kr

[2] Department of Computer Engineering, Kyung Hee University
Giheung, Yongin, Gyeonggi, 449-701 Korea
cshong@khu.ac.kr

[3] Korea Electrotechnology Research Institute
665 Nesondong, Euiwang, Gyeonggi, Korea, 437-808 Korea
jjlee@keri.re.kr

Abstract. Wireless PAN Mesh Network (WMN) is currently going to be standardized and enhanced to take full advantages of the flexible and heterogeneous networks. Although the standard (802.15.5) is under-construction, WMNs are expected to become popular as they have the ability to connect all kinds of current networks. So far, there is no applied architecture which is efficient enough to completely solve routing and security problems in WMN. To assist IEEE P805.15 in routing and security aspects, in this paper, we propose an adaptive algorithm for detecting bogus nodes when they attempt to intrude into the network by attacking routing protocol. In addition, a procedure to find the most optimal path between two nodes is presented along with adaptive pre-conditions for WMNs. We also show that our algorithm is robust according to the mobility of the nodes and it is easy to implement in currently proposed architectures. It can work with many kinds of wireless networks as well as can reduce computational costs.

Keywords: Wireless PAN Mesh Networks, Security, Intrusion Detection, Clustering, Optimal Path, Routing, Attack on Routing Protocol.

1 Introduction

Wireless Mesh Network (WMN) could be considered as a successor of the basic wireless networks such as Wireless LAN, Wireless Mobile Ad-hoc Networks (MANETs) and Wireless Sensor Networks (WSNs), which inherits full advantages of the previous ones and could be applied in many fields in daily life as well as in military operations that require dynamic topology. However, WMNs also require to deal with

[*] This work was supported by MIC and ITRC Project. Dr. C.S. Hong is the Corresponding Author.

R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops 2006, LNCS 4277, pp. 585 – 594, 2006.

inherent weaknesses of wireless networks by consequence of dynamic topologies and node mobility. Moreover, the lack of concentration points where traffic can be analyzed for intrusions leads to utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation and subject to noise and intermittent connectivity due to the inherent essence of wireless communication channels [7], [8], [9].

In WMNs, the topology is a mixture of star (with access point as coordinator) and grid (ad-hoc based) and therefore the routing protocol must be flexible for adaptive change. In our scenario, the coordinators can be mobile nodes (mobile access points or ad-hoc nodes) or station (fixed access points like WLAN access points). In this paper, we not only focus on solving routing problem of mobile nodes but also propose a mechanism to automatically work with fixed access points.

The rest of the paper is organized as follows, Section 2 briefly discusses some related works as well as addresses assigning problem which adapts to WMNs, in Section 3, we propose a procedure to find the most optimal path between two nodes when they want to communicate with each other. This procedure can be applied in any kind of wireless dynamic network. Moreover, we propose an algorithm for detecting bogus nodes when they attempt to intrude into network by attack routing protocol. Section 4 presents our simulation results. Finally, section 5 exposes some perspectives for further work.

2 Related Work

2.1 Current Work

Clustering technique is proposed in many papers for routing and formation of a dynamic topology. In security, it is also used to detect intruders. Based on the clustering technique, which was first proposed by Zhang and Lee [17], D. Sterne in [5] has given an architecture in which the author solved most of the drawbacks of a dynamic topology when implementing an Intrusion Detection System (IDS). However, as almost related papers, the author just only explained some clues to detect bogus node in routing protocol that are used to conclude that they can in principle determine whether a node is an attacker. Moreover, the authors did not specify the attributes of a node to decide whether it has enough qualifications or not to find intermediate nodes in routing protocol.

Although the proposals above are applied in MANETs, they can also be applied in the Wireless Mess Networks that are with almost same dynamic topology by making some slight modifications to routing protocol. As we know, the attack in routing protocol is very hard to prevent, especially in the wireless environment where the traffic can be easily eavesdropped, therefore we improve current contributions by taking advantages of previous proposals and using them as building blocks for our proposals. In this paper, AODV (Ad hoc On-demand Distance Vector) [18], [19], an adaptive protocol, is also utilized in our work.

Currently, the IEEE P802.15 Working Group for WPANs has been making a standard for WMNs with many achievements [1], [2]. In those proposals, they also used mesh tree, another form of cluster, to solve almost problems in routing. However, they did not focus on security for routing, as well as giving a solution to finding optimal path between two nodes. Our proposal is a contribution for completing the 802.15.5 standard in aspect of routing and security.

2.2 Address Assigning Problem

Cluster-tree technique can be applied in any kind of network that has dynamic topology. In the cluster-tree, a node can have a maximum number of C_M children and a node can be at most L_M levels (i.e., mobile devices) away from the root of the tree (C_M and L_M are two predetermined network-wide constants). A node with a short address s is in charge of assigning short addresses to its children as in the following algorithm [16]: assign short address s+1 to the first child, s+1+$C_{hold}(L_N)$ to the second child, and s + 1 + (n - 1).$C_{hold}(L_N)$ to the nth child, up to the (C_M)th child. And $C_{hold}(L_N)$ is calculated as follows:

$$C_{hold}(L_N) = \left\lfloor \frac{T - \sum_{k=0}^{L_N} (C_M)^k}{(C_M)^{L_N+1}} \right\rfloor$$

$$T = \sum_{k=0}^{L_M} (C_M)^k$$

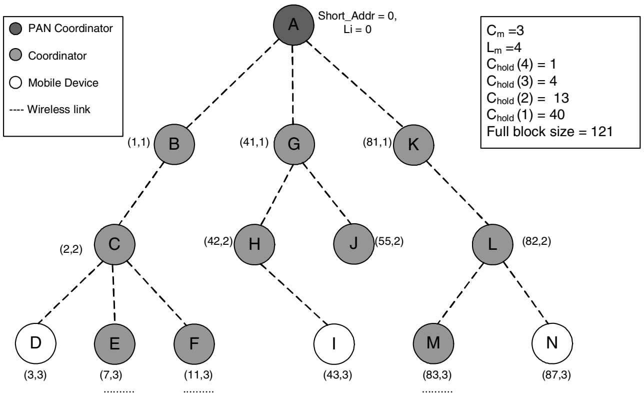

Fig. 1. Assigning Address

In which:

T : Address Block Size

$C_{hold}(L_N)$: Number of address each node of specific level can hold

L_N : Level of Node

C_M : Maximum number of children of a specific level node

L_M : Maximum level in a cluster-tree

After executing some mechanisms to establish and maintain the dynamic topology as well as to choose the coordinator, this coordinator begins to accept association requests from other nodes. Any node already existent in the network can determine whether to allow other nodes to join to the network, that is, whether to act as a coordinator, depending on the availability of its resources such as memory and energy. In a cluster-tree, a node is able to calculate the next hop by looking at the destination address in the packet. This precludes the need of route discovery, and thus helps reduce the initial latency, control overhead, memory usage and energy consumption.

In the Figure 1, an example of assigning address is given with L_M=4, C_M=3. It means the coordinators in level3 only have maximum 3 children (mobile terminals), and the rest of the remaining nodes can be assigned their own address as well as their holding address block size which rely on the level of nodes.

3 Proposed Algorithms

The hybrid topology of WMNs makes their routing problem more difficult than homogeneous networks. In this case, we need a routing protocol that can work in two network structures: Mobile nodes with fixed Access Point (as Coordinator) and entirely mobile nodes (Ad-hoc topology)

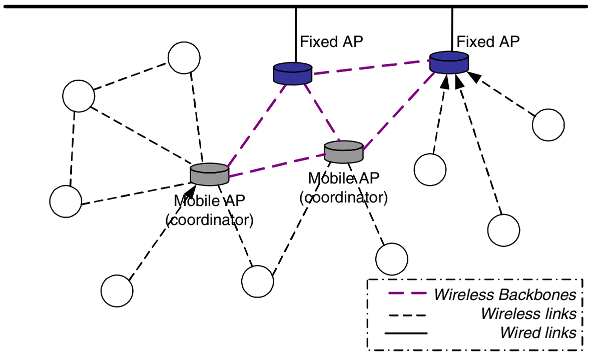

Fig. 2. Mesh Topology

In the previously proposed cooperative intrusion detection architecture using clustering technique [5], the authors presented their solutions to detect attack on routing protocol, but they did not give any algorithm to prove that their technique can detect and exclude bogus nodes. Furthermore, they did not also give any procedure with specific criteria to find the shortest (the most optimal) path.

In this paper, we do two jobs: the first one is proposing a procedure to find a shortest (the most optimal) path using three most important criteria, signal strength, bandwidth and energy remaining. The other is proposing mechanism to identify and exclude bogus nodes.

To implement our proposal, some pre-conditions are established.

We use the clustering technique to establish and maintain the dynamic hierarchy according to node mobility. We also use AODV (Ad hoc On-demand Distance Vector) as routing protocol in our proposal. In addition, for hybrid structure in WMNs, we propose some small changes in routing protocol:

1. When two nodes in the ad-hoc part of WMNs want to communicate with each other, they use Multicast Routing Protocol [1] with our adaptively proposed procedure presented below.
2. When one node in ad-hoc part wants to communicate with others in fixed Access Point (AP) part, it finds the AP where the destination is currently connect with and after that can transfer data through this AP.
3. When two nodes in the fixed AP part of WMNs want to communicate with each other, their current APs will act as intermediate nodes and use our proposed procedure to find shortest path.

3.1 Optimal Path Finding Algorithm

There are many criteria to decide whether a node has ability and capacity to become an intermediate node in a route. In such a dynamic topology like WMNs, it is very difficult to find a completely good routing protocol which can automatically reform and maintain connection. The most three important criteria we use in our procedure are *Signal strength*, *Bandwidth,* and *Energy Remaining* because they guarantee for a stable and high-speed connection. When a node wants to communicate with another one, the following steps are processed:

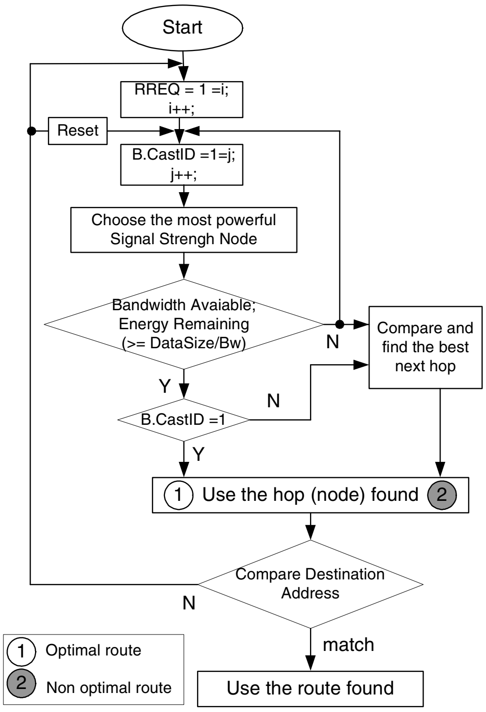

Fig. 3. The Most Optimize Path Procedure

Step 1: Initial RREQ = 1, BroadcastID = 1, the source node floods RREQS packets with destination address to its neighbors and chooses the node with the most powerful signal strength.

Step 2: Estimate the available Bandwidth and Energy Remaining of this node, if its free bandwidth ≥ 50% & If necessary time >= DataSize/Bandwidth

Choose this node as a next hop

Else, repeat *Step 1* to choose another node, remember information of current node to compare with new found node to find the most optimistic node. B.CastID++;

End if

```
    Step 3: If Node's B.CastID = 1
    Use the found node
Else, use this node to compare with previous found node and choose the best one.
    Step 4: Compare Destination Address
If found Node's Address is the same as Destination Address, go to Step 5
Else { repeat Step 1; Reset B.CastID = 1; }
    Step 5: Choose the route
Finish
```

In Step 2, the available bandwidth is assigned ≥ 50%. This value can be adjusted to suit requirement in a specific network. If a node with the highest signal strength and enough bandwidth is found in each hop, along with enough energy remaining, it means the optimal route is found. If not, we can also find the best route at the final part of Step 3. Available bandwidth and energy remaining can be easily estimated in nodes themselves with current softwares.

In Step 3, the sender has known the size of the packet that it intends to transmit to receiver. In addition, with currently available bandwidth (can be evaluated by each node itself in the route), the necessary time can be calculated and compared with the remaining energy time of each node in the route. Based on the requirements of network, we can add other criteria such as proximity, resistance to compromise, accessibility, processing power, storage capacity, etc. to the procedure.

If a node in the route satisfies all conditions in the procedure, that node is an optimal one. If a route has all optimal intermediate nodes, it is called optimal route.

3.2 Identify and Exclude Bogus Nodes

This algorithm is used to detect and exclude intruders at any time they attempt to break routing mechanism.

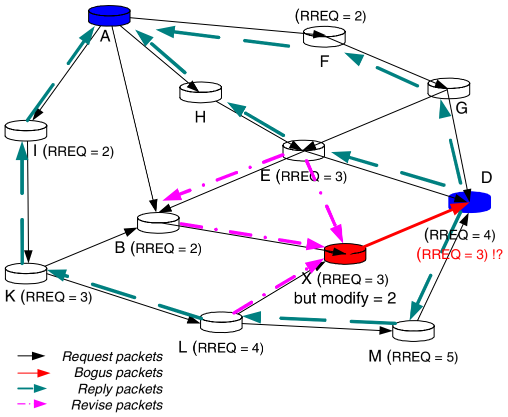

Fig. 4. Identify Bogus Node

```
Initial
$RREQ_S = 1$, $RREP_D = 0$, Found Route Count = 0;
flood $RREQ_S$ in the network topology;
for each time $RREQ_S$ reaches node i
do RREQi = RREQi + 1;
$N_{hop\,i}$ = RREQi;
compare destination address;
if destination found
do Co-revise Procedure
    {
    for each route found from S to D
    Found Route Count++;
   send $RREP_D$ back through other routes different from route of the first reach RREQ packet;
    $RREP_{Dj} = N_{hop\,j} - j$;
    compare (RREQj , RREPj) index;
    if RREPj index determined by neighbor nodes $\neq$ RREQj index;
    trigger an alarm;
    }
exclude j out of connection;
Finish
```

The number of routes found is counted by Found Route Count and is stored in routing table to help routing protocol distinguish different routes, decide which routes are chosen and keep the information for optimal path finding as well as back-up purpose.

To avoid bogus nodes from modifying RREP packets before sending them back to the same route, the destination node will send RREP packets through other routes. By this way, Co-revise Procedure can completely identify intruders. The number of backward routes is limited to avoid redundancy and reduce the number of nodes involved in routing procedure. At least two neighbors of bogus node X will ensure that X is intruder, after comparing RREQ index that X modified with its real RREQ by the following revising mechanism:

Assume X is attacker and it is trying to access to the route between A and D. Following the procedure, $RREQ_A = 1$, A floods its request to find optimal route to D. In the figure 4, $RREQ_{B, H, F, I} = 2$ because they are neighbors of A, and $RREQ_{G, E, K} = 3$ and so on until the RREQ reaches D. If X is a legal node and it is in network topology, $RREQ_X$ must be 3, but it modified this index, suppose $RREQ_X = 2$, and sends to D. In principle, D will “think” the route include X is optimal, and choose this route.

But now D can use proposed algorithm above, send back RREP to the other routes, like D-E-H-A and D-G-F-A. After that, B and E can themselves calculate the real RREQ index of X, and find it have to logically equal 3. Also, if $RREQ_X = 2$, it means X have to be a neighbor of A like B,E,F, but A can itself determine C is not a neighbor because A can not directly communicate with X. In brief, the algorithm can definitely detect X is intruder, trigger an alarm and exclude X out of network.

In the Figure 4, we can see path A-I-K-L-M-D is also exist, but destination node D will not use it because the number of intermediate nodes is large. The routing protocol in [1] has already solved this problem. Therefore, D will not send back $RREP_D$ through this path and thereby limiting the number of nodes have to involve in routing protocol. This mechanism also help our proposals save energy, reduce time consumption and memory usage.

4 Simulation Result

Our proposed algorithm is simulated to further evaluate the theoretical results. We use OMNeT++ Ver.3.2 with Mobility Framework 1.0a5 Module. We present each node as a matrix in which attributes (*Signal Strength, Band Width, Energy Remaining, Address, etc.*) are assigned as factors. We use routing table in [1] with additional fields *Found Route Count* and *Sequence Number*. We also set up a mobility environment to evaluate the performance in detection rate and calculation time influenced by different movement speed of nodes. The nodes have radio range of 300m and move on the rectangular surface according to the boundless mobility model. We study the detection rate, cardinality and time consuming according to mobility and network cardinality.

In the figure 5, the detection rate of bogus nodes is 99.05% for a set of 25 nodes at speed 5m/s and. The detection rate is a little bit decrease according to the increase of

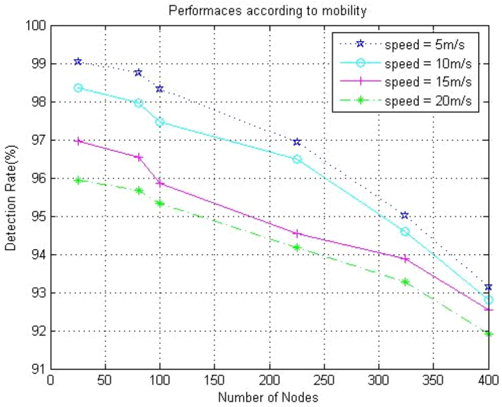

Fig. 5. Performance according to mobility

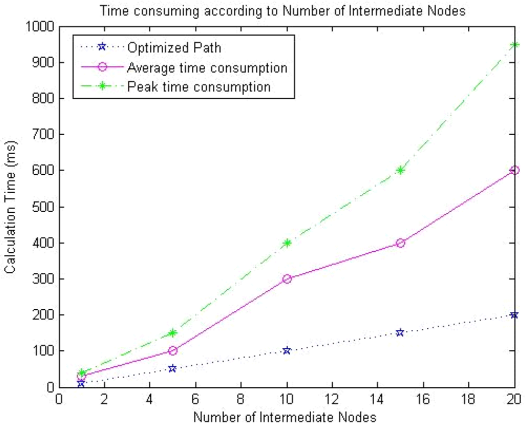

Fig. 6. Time consumming

number of nodes as well as speeds. At speed 20m/s and 400 nodes, the detection rate is reduced to 91.92%.

In figure 6, the time consuming for finding intermediate nodes in case of optimal path is also the least. It is directly proportional to the numbers of intermediate nodes. We evaluate the peak of calculation time and average time in case of non-optimal path.

5 Conclusion and Future Work

Our proposed approach in this paper bases on dynamic topology maintained by clustering technique, uses AODV as the routing protocol, inherits the achievements of previous researchers and improve shortcomings in their proposals. By making adaptive changes, our algorithm can be applied to any kind of Wireless Network such as WMNs, MANETs and WSNs. To apply our algorithm, we just insert additional fields Found Route Count and Sequence Number into routing table. The simplicity of our algorithm is that it does not require a considerable amount of computational resource, even there are a large number of nodes in a selected route. Each time the algorithm find the next hop, the process returns to the initial point at Step 1 and does the same jobs until the destination is found. Consequently, the number of times that needed to process is direct proposition with the number of intermediate nodes in route, and the complexity in each Step is trivial.

Moreover, our proposals can work with currently used protocols and completely solved routing problem for nodes in different wireless networks.

In future works, we will continue implementing our proposal in Testbed cooperating with current Intrusion Detection Systems (IDSs) for Wireless Networks. Furthermore, we are working on an algorithm for automatic reforming topology based on clustering technique which will run in company with our proposals.

References

1. IEEE 802.15-15-05-0247-00-0005, “Mesh PAN Alliance (MPA)”, IEEE 802.15.5 Working Group for Wireless Personal Area Networks.
2. IEEE 802.15.5-05-0260-00-0005, “IEEE 802.15.5 WPAN Mesh Network”, IEEE 802.15.5 Working Group for Wireless Personal Area Networks.
3. Guan, Y. Ghorbani, A. Belacel, “A clustering method for intrusion detection”. Proceedings of Canadian Conference on Electrical and Computer Engineering, 1083-1086, Canada, 2003.
4. Stefano Basagni, “Distributed Clustering in Ad Hoc Networks”, Proceedings of the 1999 Intl. Symp. On Parallel Architectures, Algorithms and Networks (I-SPAN ’99), Freemantle, Australia, 1999.
5. 5. D.Sterne, “A General Cooperative Intrusion Detection Architecture for MANETs”, Proceeding of the Third IEEE International Workshop on Information Assurance (IWIA’05), 0-7695-2317-X05 IEEE, 2005.
6. Yi-an Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) George W. Johnson Center at George Mason University, USA, October 31, 2003.
7. Vesa Karpijoki, “Security in Ad Hoc Networks” http://citeseer.nj.nec.com/karpijoki01security.html
8. P. Brutch and C. Ko, “Challenges in Intrusion Detection for Ad Hoc Network”, IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
9. Konrad Wrona, “Distributed Security: Ad Hoc Networks & Beyond”, PAMPAS Workshop, London, Sept. 16/17 2002.
10. F. Theoleyre, F. Valois, “A Virtual Structure for Hybrid Networks”, IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, USA, March 2004.
11. P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan, “A cluster-based approach for routing in dynamic networks”, ACM SIGCOMM Computer Communication Review, 1997.
12. M.-Y. Huang, R. J. Jasper, and T. M. Wicks, “A large scale distributed intrusion detection framework based on attack strategy analysis”, Computer Networks, pp. 2465–2475, 1999.
13. Jake Ryan, Meng-Jang Lin, Risto Milikkulainen, “Intrusion Detection with Neural Networks”, Advances in Neural Information Processing Systems 10 (Proceedings of NIPS'97, Denver, CO), MIT Press, 1998.
14. K. Ilgun, R. A. Kemmerer, and P. Porras, “State transition analysis: A rule-based intrusion detection approach”, IEEE Trans on Software Engineering, pp. 181–199, 1995.
15. P. A. Porras and P. G. Neumann, Emerald, “Event monitoring enabling responses to anomalous live disturbances”, in Proc of 20th NIST-NCSC Nat’l Info Systems Security Conf, pp. 353–365, 1997.
16. Jianliang Zheng, Myung J. Lee, Michael Anshel, “Towards Secure Low Rate Wireless Personal Area Networks”, IEEE Transactions on mobile computing.
17. Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks”, Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, August 2000.
18. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF RFC 3561.
19. C. E. Perkins and E. M. Royer, “The ad hoc on-demand distance-vector protocol”, In C. E. Perkins, editor, Ad Hoc Networking. Addison-Wesley, 2000.