DETECTION OF INTRUDER NODE IN AUTONOMOUS MOBILE MESH NETWORK

S.KANAGARAJ
II-ME (Communication & Networking)
Department of Electronics and Communication Engineering,
Sengunthar College of Engineering,
Tirunchengode – 637 205

Mr. N. KIRAN KUMAR SUBHASH, M.E.
Assistant Professor
Department of Electronics and Communication Engineering,
Sengunthar College of Engineering,
Tirunchengode – 637 205.

ABSTRACT—In this paper Autonomous Mobile Mesh Network with security. In Mobile Adhoc Network nodes move from one place to another place in free directions. The movement of the nodes may split the network and form more than one group. In this case communication between two nodes will be disconnected. To maintain the communication between all nodes even they are in different groups Mesh Nodes are used. Mesh Nodes which have the capability of changing its nature into Inter-group router or Intra-group router. Even it can act as a bridge router. To make the communication effective One-hop neighbor information update is used to find the shortest path between any two nodes. Since nodes move from one place to another place intruder may join the group. To avoid this problem private key is assigned for all the nodes in the network and it is shared among the nodes. If any node want to communicate with the other node first private key must be exchanged. Only if private key matches nodes can communicate. If key does not matches then the node ID will be registered in the Blacklist. If any node registered in the blacklist says the private key wrongly, then the node will be removed from the network. In this way security can be provided to the network. Now a Days MANETs, however, may suffer from network partitioning. This limitation makes MANETs unsuitable for applications such as crisis management and battlefield communications, in which team members might need to work in groups scattered in the application terrain. A new cryptographic algorithm is developed to improve the time for encryption and decryption of data of end-to-end delay and provide higher level of security.

I. INTRODUCTION

WIRELESS technology has been one of the most transforming and empowering technologies in recent years. In particular, mobile ad hoc networks (MANETs) are among the most popularly studied network communication technologies. In such an environment, no communication infrastructure is required. The mobile nodes also play the role of the routers, helping to forward data packets to their destinations via multiple-hop relay. This type of network is suitable for situations where a fixed infrastructure is unavailable or infeasible. They are also a cost effective solution because the same ad hoc network can be relocated, and reused in different places at different times for different applications.

One great challenge in designing robust MANETs is to minimize network partitions. As autonomous mobile users move about in a MANET, the network topology may change rapidly and unpredictably over time; and portions of the network may intermittently become partitioned. This condition is undesirable, particularly for mission-critical applications such as crisis management and battlefield communications. We address this challenging problem in this paper by proposing a new class of robust mobile ad hoc network called Autonomous Mobile Mesh Networks (AMMNET).

In a standard wireless mesh network, stationary mesh nodes provide routing and relay capabilities. They form a mesh-like wireless network that allows mobile mesh clients to communicate with each other through multihop communications. Such a network is scalable, flexible, and low in maintenance cost.

II. LITERATURE REVIEW

Robust Positioning Algorithms for Distributed Ad-HocWireless Sensor Networks [1]. Ad-hoc wireless sensor networks are being developed for use in monitoring a host of environmental characteristics across the area of deployment, such as light, temperature, sound, and many others. Most of these data have the common characteristic that they are useful only when considered in the context of where the data was taken from, and so most sensor data will be stamped with position information. As these are ad-hoc networks, however, acquiring this position data can be quite challenging. In this paper we have presented a completely distributed algorithm for solving the problem of positioning nodes within an ad-hoc, wireless network of sensor nodes.

© 2014- 16, IJIRAE- All Rights Reserved

The procedure is partitioned into two algorithms: Hop- TERRAIN and Refinement.Each algorithm is described in detail. The simulation environment used to evaluate these algorithms is explained, including details about the specific implementation of each algorithm. Many experiments are documented for each algorithm, showing several aspects of the performance achieved under many different scenarios. Finally, guidelines for implementing and deploying a network that will use these algorithms are given and explained. An important aspect of wireless sensor networks is energy consumption. In the near future we therefore plan to study the amount of communication and computation induced by running Hop-TERRAIN and Refinement. A particularly interesting aspect is how the accuracy vs. energy consumption trade-off changes over subsequent iterations of Refinement.

Robust Positioning Algorithms for Distributed Ad-Hoc Wireless Sensor Networks [2]. Ad-hoc wireless sensor networks are being developed for use in monitoring a host of environmental characteristics across the area of deployment, such as light, temperature, sound, and many others. Most of these data have the common characteristic that they are useful only when considered in the context of where the data was taken from, and so most sensor data will be stamped with position information. As these are ad-hoc networks, however, acquiring this position data can be quite challenging. In this paper we have presented a completely distributed algorithm for solving the problem of positioning nodes within an ad-hoc, wireless network of sensor nodes. The procedure is partitioned into two algorithms: Hop- TERRAIN and Refinement. Each algorithm is described in detail. The simulation environment used to evaluate these algorithms is explained, including details about the specific implementation of each algorithm. Many experiments are documented for each algorithm, showing several aspects of the performance achieved under many different scenarios. Finally, guidelines for implementing and deploying a network that will use these algorithms are given and explained. An important aspect of wireless sensor networks is energy consumption. In the near future we therefore plan to study the amount of communication and computation induced by running Hop-TERRAIN and Refinement. A particularly interesting aspect is how the accuracy vs. energy consumption trade-off changes over subsequent iterations of Refinement.

Interference-Aware Channel Assignment in Multi-RadioWireless Mesh Networks [3]. This paper presents an interference-aware channel assignment algorithm and protocol for multi-radio wireless mesh networks that address this interference problem. The proposed solution intelligently assigns channels to radios to minimize interference within the mesh network and between the mesh network and co-located wireless networks. It utilizes a novel interference estimation technique implemented at each mesh router. An extension to the conflict graph model, the multi-radio conflict graph, is used to model the interference between the routers. We demonstrate our solution’s practicality through the evaluation of a prototype implementation in a IEEE 802.11 test bed. We also report on an extensive evaluation via simulations. In a sample multi-radio scenario, our solution yields performance gains Multi-radio routers can significantly improve the performance of wireless mesh networks.However, any static assignment of channels to the mesh radios can degrade network performance because of interference from co-located wireless networks. This paper presented BFS-CA, a dynamic, interference aware channel assignment algorithm and corresponding protocol for multi-radio wireless mesh networks. BFS-CA improves the performance of wireless mesh networks by minimizing interference between routers in the mesh network and between the mesh network and co-located wireless networks. The proposed solution is practical and easily implementable. We find that BFS-CA results in significant performance improvements in the presence of varying interference levels, which are validated through empirical measurements on a test bed. As future work, we plan to evaluate BFS-CA on the UCSB Mesh Net, a thirty node multi-radio wireless mesh test bed at UCSB.

Lifetime and Coverage Guarantees through Distributed Coordinate-Free Sensor Activation [4]. The contribution of this paper is two-fold. First, we present the rest coordinate-free distributed scheme that provides provable approximation guarantees on network lifetime, while providing strict coverage guarantees. This is a surprising result since the sensors are not aware of their coordinates in a global coordinate system, and are there- fore oblivious to their locations relative to each other and to the target end. To overcome this challenge we assume that the sensor distribution area is slightly larger than the area that needs to be monitored. The sensors are divided into periphery nodes that are located near the boundary of the distribution area and internal nodes that are internal to this area. The target end that our scheme is committed to monitor is taken as the closure of the area covered by the internal nodes. Our scheme at each time slot selects a subset of sensors for monitoring the target end that ensure *K*-coverage of the entire target end, for a given integer *K* ¸ 1, and different subsets may be selected in different slots. The selection process relies on two key steps: Each sensor is assigned a weight that is an exponentially increasing function of the energy it has consumed so far. The set of sensors that has the minimum total weight, or an approximation thereof, among all those that cover the entire target end is activated. This selection process balances the monitoring load on all the sensors, and preferentially selects in each slot the sensors with high residual energy.

© 2014- 16, IJIRAE- All Rights Reserved

We demonstrate that the algorithm can be executed using distributed computations that do not need to know the locations of the sensors.

Topology Control and Channel Assignment in Multi-RadioMulti-Channel Wireless Mesh Networks [5]. The aggregate capacity of wireless mesh networks can be improved significantly by equipping each node with multiple interfaces and by using multiple channels in order to reduce the effect of interference. Efficient channel assignment is required to ensure the optimal use of the limited channels in the radio spectrum. In this paper, a Cluster-based Multipath Topology control and Channel assignment scheme (CoMTaC), is proposed, which explicitly creates a separation between the channel assignment and topology control functions, thus minimizing flow disruptions. A cluster-based approach is employed to ensure basic network connectivity. Intrinsic support for broadcasting with minimal overheads is also provided. CoMTaC also takes advantage of the inherent multiple paths that exist in a typical WMN by constructing a spanner of the network graph and using the additional node interfaces.

The second phase of CoMTaC proposes a dynamic distributed channel assignment algorithm, which employs a novel interference estimation mechanism based on the average link-layer queue length within the interference domain. Partially overlapping channels are also included in the channel assignment process to enhance the network capacity. The cluster-based topology of CoMTaC ensured basic network connectivity with intrinsic support for broadcast. Multipath topology was constructed which took advantage of the inherent multiple paths that exist in a typical WMN by constructing a spanner of the network graph. The dynamic distributed channel assignment scheme of CoMTaC employed a novel interference estimation mechanism based on the average link-layer queue length within the interference domain. The simulation based experiments showed that CoMTaC outperformed the base case of single channel WMN by a factor of at least 5.

III. OVERVIEW OF THE STUDY

Similar to stationary wireless mesh networks, an AMMNET is a mesh-based infrastructure that forwards data for mobile clients. A client can connect to any nearby mesh node, which helps relay data to the destination mesh node via multihop forwarding. For ease of description, in this paper we use the terms “mesh node” and “router” interchangeably. Like stationary wireless mesh networks, where routers are deployed in fixed locations, routers in an AMMNET can forward data for mobile clients along the routing paths built by any existing ad hoc routing protocols, for example, AODV. Unlike stationary wireless mesh networks, where routers are deployed at fixed locations, routers in an AMMNET are mobile platforms with autonomous movement capability.. They are equipped with positioning devices such as GPS, to provide navigational aid while tracking mobile clients. Clients are not required to know their locations, and only need to periodically probe beacon messages. Once mesh nodes receive the beacon messages, they can detect the clients within its transmission range. With this capability, mesh nodes can continuously monitor the mobility pattern of the clients, and move with them to provide them seamless connectivity. Intragroup routers. A mesh node is an intragroup router if it detects at least one client within its radio range and is in charge of monitoring the movement of clients in its range. Intragroup routers that monitor the same group of clients can communicate with each other via multihop routing. For example, routers r_1 and r_2 in F are intragroup routers that monitor group G_1. Intergroup routers. A mesh node is an intergroup router, i.e., square nodes , if it plays the role of a relay node helping to interconnect different groups. For each group, we designate at least one intergroup router that can communicate with any intragroup routers of that group via multihop forwarding as the bridge router, for example, router b_1 for group G_1.Free routers. A mesh node is a free router if it is neither an intragroup router nor an intergroup router.

IV. TECHNIQUES

Adapting to Intragroup Movement[1].We recall that each client continuously broadcasts beacon message to notify its present within the ratio range of an intragroup router. When this router no longer hears the expected beacon messages, one of two possible scenarios might have happened. The first scenario is illustrated. It shows that client c moves out of the communication range of router r into the communication range of an adjacent router r^0 in the same group. The second scenario is illustrated in Fig. 5b. It shows that the missing client c moves from the communication range of router r to a space not currently covered by any of the routers in the group. The router r can distinguish the above two scenarios by querying its neighboring routers for their lists of monitored clients. If c is in any of these lists, r determines that the first scenario has occurred. In this case, since some of the neighboring routers provide the coverage for c, no further action is required. On the other hand, if none of the client lists includes c, which indicates the second scenario, topology adaptation is required to extend the coverage to include c at its new location.

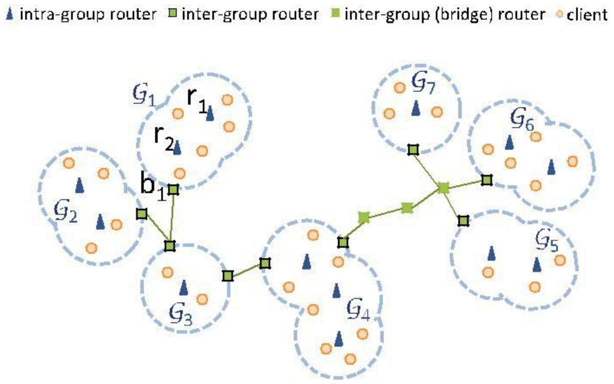

Fig. 1. AMMNET Framework. Routers are partitioned into two groups. Intragroup routers support intragroup communication; and intergroup routers prevent a network partition.

Topology adaption[2].The protocol discussed so far ensures that the mesh nodes maintain the connectivity for all clients. The resulting networks, however, might incur long end-to-end delay with potentially many unnecessary intergroup routers because the bridging networks are constructed independently. As the example shown in Fig. 6c, if a client in group G_2 wants tocommunicate with another client in group G_3, this must be done through a long path over the router b_1 at group G_1 although groups G_2 and G_3 are near each other. Another potential drawback is the excessive use of the intergroup routers. To improve this condition, we propose two topology adaptation schemes, namely local adaptation and global adaptation, each with a different resolution of location information to shorten the relay paths between groups.

Local Adaption[3].Consider again the example in Fig. 6c. To save intergroup routers, we can replace three independent bridging net-works with a star network. A star topology generally provides shorter relay paths, and, as a result, requires fewer intergroup routers. To construct a star topology, we let the bridge routers exchange their location information opportunistically, and perform local adaptation as shown in Algorithm 2 when some bridge routers detect that they are close to each other.

Algorithm 2. Topology Adaptation (initiated by router r). input: (Collected in Algorithm 1) R_b: set of bridge routers known by r opportunistically; L_b: location of router b 2) R_b; R_i: set of intergroup routers connecting all known bridge routers b 2 R_b

```
if number of free routers in r's group < _ then
    Call Algorithm 3 to perform global adaptation;
else
    Compute the single star topology S for $R_b$;
    Build a bridge network B connecting to any bridge
    router $b^0$ 62 $R_b$;
    $N_i^0$      number of intergroup routers needed for
    Sand B;
    if $N_i^0$ _ _j$R_i$j then
        Trigger the assigned intergroup routers to adapt
          their topology to S [ B after a three-way handshaking;
        Reclaim the rest of intergroup routers to the free-router poor;
    end if
end if
return
```

Specifically, when clients in different groups are communicating with each other, the corresponding bridge routers can exchange their location information by piggy-backing such information in the data packets.

Global Adaptation[4]. Local topology adaptation provides local optimization. It is desirable to also perform global topology adaptation to achieve global optimality. The motivation is to achieve better overall end-to-end delay and free up intergroup routers for subsequent local adaptation.

© 2014- 16, IJIRAE- All Rights Reserved

A simple option for global optimization is to apply Algorithm 2 to construct a star network for all the bridge routers in the AMMNET. Such a star network, however, would be inefficient and require more intergroup routers than necessary, particularly when there are a significant number of groups in the network.

Ideally, an AMMNET should use as few intergroup routers as possible to minimize the number of mobile routers required and deliver good end-to-end delay for the application. This optimization problem can be formulated as the connected set cover problem, which has been proved to be NP-hard [14], [15]. In this paper, we propose a hierarchical star topology, which is a near-optimal techni-que based on R-tree [16] as shown in Algorithm 3. The R-tree is a multidimensional tree structure that aggregates at most M objects into a minimum-bounding rectangle. M of such rectangles are further aggregated into a larger bounding rectangle at the next higher level in the tree. This clustering process is repeated recursively at the higher levels until there is a single minimum-bounding rectangle left at the root of the R-tree. To determine a suitable value of M, we can apply k-means clustering or affinity propagation to cluster the bridge routers in the network. The latter does not require a specified number of clusters k. After clustering, each bridge router is associated with a distinct cluster based on its Euclidian distance with the centroid of the cluster. M is determined as the average.

size of all the clusters, i.e., M ¼ $^{Pk¼}_{i}$ $_{1}$ jC^{i}j=k, where k is the number of clusters and jC$_{i}$j is the number of bridge routers in the ith cluster C$_{i}$.

Algorithm 3. Hierarchical Star Topology Construction. Input: M: size of a bounding box

```
Broadcast a message to all the bridge routers to collect information and coordinate global adaptation;
Rb      set of bridge routers;
$L_b$      location of routerb 2 $R_b$;
Ri      set of nonbridge intergroup routers;
Classify all r 2 $R_b$ into cluster $C_i$; i ¼ 1; 2; . . . ; k;
M      $^{jC}_{k}$i$^{j}$ ;
T      R-Tree($R_b$; $L_b$; M);
for all vertex v in T do
    while v is a leave node and any $r_i$; $r_j$ 2 v belong to the same group do
        Remove $r_j$ from v;
    end while
    if not all elements r 2 v are interconnected then
        Deploy a subset of intergroup routers in $R_i$ as a star topology to connect all r 2 v and remove those routers from $R_i$;
    end if
end for
Reclaim the remaining routers in $R_i$ as free routers;
return
```

V. EVALUATION

We conduct extensive simulations, implemented via NS2 , to study the ability of AMMNET in adapting to the dynamic movement of mobile clients and the data forwarding efficiency of such networks. Our performance evaluation compares the following network schemes:

Grid-mesh. This simple scheme employs a grid based square topology for the mobile mesh nodes. This mobile mesh network follows the users by tracking and following one randomly selected client. The network maintains the same grid topology as it moves over the application terrain.

AMMNET. This is our design of AMMNET, in which routers adapt their locations using only locally cached location information about some of the bridge routers. Global adaptation is also performed when the number of free routers at some user groups drops below a predefined threshold.

Global-AMMNET. This is similar to the above AMMNET, except that global adaptation is per-formed by a randomly selected bridge router whenever any client moves out of the current network coverage area.

Oracle. This is a centralized scheme that assumes location information of all clients is available. The routers can move to the assigned locations in the network instantaneously without any moving delay. This scheme is only used as a bound for the purpose of performance comparison. Unlike AMMNET that uses the locations of the bridge routers to approx-imate the distribution of the user groups in the application terrain and constructs the R-tree based on these routers accordingly, Oracle constructs the R-tree using the exact locations of the mobile users. When there are not enough available routers to provide full connectivity for all the clients, this scheme favors user groups (R-tree nodes) with a higher density of clients.

Unless stated otherwise, we use the following default values for the parameters. In each simulation, all clients originate from a randomly selected initial region in the terrain. These clients belong to several mobile groups. The number of clients in each group follows a Zipf distribution. Members of each user group demonstrate the following group mobilitypattern the group leader moves in accordance to the random way-point mobility model with a moving speed that is uniformly distributed with a mean of 2.5 m/s; and the group members follow the leader with their own random local movements. There are 200 mesh nodes; and we assume the AMMNETs are airborne, with the flying wireless routers implemented using devices such as quadrocopters.

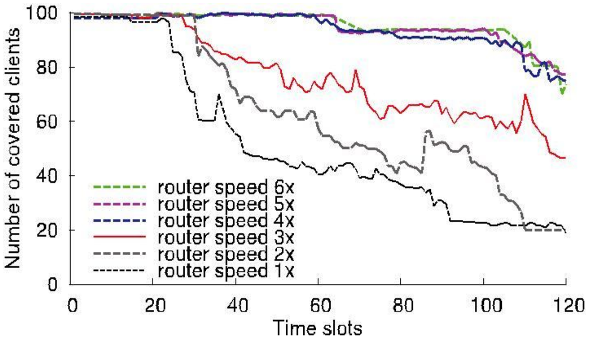

Fig. 2. Impact of router speeds: 4_ is sufficient to track mobile clients.

Their flying speed, which is within the device’s normal operating capability range is 10 m/s. Their communication range is 150 m. However, since they are flying at a height of 90 m, the coverage radius of each router is reduced to 120 m on the ground. Each simulation run continues for 120 time slots of 10 seconds each. In each time slot, five pairs of clients are randomly selected to transmit UDP traffic. Each router applies AODV to build its routing table. The simulation results reported in this paper are averaged over 20 simulation runs.

VI .PERFORMANCE DATA FORWARDING

We next examine the throughput performance in a critical environment, where the number of mesh nodes is not sufficient to always provide full coverage. As a result, we set the number of available routers to 125 because the result in Fig. 10 shows that the number of routers required to cover all clients is about 130 on average. In this simulation, we also compare AMMNET with the traditional mobile ad hoc network. Since MANET is not an infrastructure-based network, we let each MANET user act as a mobile router, which can transmit/receive its own data and also forward data for other users. Each simulation includes 100 clients partitioned into five mobility groups. Each router forwards data at the transmission bit-rate of 11 Mb/s. From the 60th to 90th time slots, we randomly select five pairs of nodes to concurrently transmit UDP flows, each with a data rate of 800 Kb/s.To isolate the impact of frequent route update on the forwarding throughput, we measure the throughput of Oracle only when the routing table in each router has been reconfigured after each topology adaption. Nevertheless, the throughputs of all the other schemes are measured for the entire duration of the simulation to evaluate how they are affected by dynamic topology and route reconfiguration.

The average throughput of all the traffic given various numbers of mesh nodes.[1] The figure shows that the average throughput obtained in AMMNET is about 33 percent higher than that in the grid-based mesh. This is due to the fact that some source-destination pairs in the grid-based mesh are not served by any routers and data could not be delivered.

© 2014- 16, IJIRAE- All Rights Reserved

AMMNET can achieve a through-put about 70 percent of that of the Oracle scheme. The performance gap comes from the slightly longer relay paths, and, more deterministically, the packet loss due to route reconfiguration. More specifically, when mesh nodes adapt their locations to client movements, each router cannot relay data along the previous relay paths and needs to discover new routes. Some packets buffered in the original routing paths might be dropped, resulting in throughput degradation. Moreover, the throughput of MANET is far lower than that of AMMNET. This is to be expected because, when the network is partitioned into multiple groups, a MANET source destination pair might not be able to find a path to communicate with each other when they belong to two partitioned groups, as a result leading to a zero throughput. This situation is quite common in a dynamic environment.

VII. SYSTEM OVERHEAD

To perform network adaptations, a node needs to collect location information of the bridge routers, and multicast the assigned locations to the selected intergroup routers. In this study, we evaluate the number of exchanged messages required for such an adaptation process. Here, each message forwarding over a wireless link is counted as a message exchange. We consider a network with 100 users and 200 routers. The Grid-Mesh schemes are excluded in this study because each mesh node only needs to notify its updated location to it neighboring nodes. Namely, in Grid-Mesh, the message overhead is independent of the number of groups in a terrain.

The Autonomous Mobile mesh network with security. In MANET nodes move from one place to another place in free directions. The movement of the nodes may split the network and form more than one group. In this case communication between two nodes will be disconnected. To maintain the communication between all nodes even they are in different groups Mesh Nodes are used. Mesh Nodes which have the capability of changing its nature into Inter-group router or Intra-group router. Even it can act as a bridge router. To make the communication effective One-hop neighbour information update is used to find the shortest path between any two nodes. Since nodes move from one place to another place intruder may join the group. To avoid this problem private key is assigned for all the nodes in the network and it is shared among the nodes. If any node want to communicate with the other node first private key must be exchanged. Only if private key matches nodes can communicate. If key does not matches then the node ID will be registered in the Blacklist. If any node registered in the blacklist says the private key wrongly, then the node will be removed from the network. In this way security can be provided to the network.Advantages of Proposed System:One-hop neighbor information update is used for finding the shortest path and Secret key is maintained for providing security to the network. Free routers help to find the missing node.

VIII. CONCLUSION

For applications such as crisis management and battlefield communications, the mobile users need to work in dynamically formed groups that occupy different parts of a large and uncertain application terrain at different times.In this paper, we introduced a mobile infrastructure called AMMNET. Unlike conventional mobile ad hoc networks that suffer network partitions when the user groups move apart, the mobile mesh routers of an AMMNET track the users and dynamically adapt the network topology to seamlessly support both their intergroup and intergroup communications. Since this mobile Infrastructure follows the users; full connectivity can be achieved without the need and high cost of providing Network coverage for the entire application terrain at all time as in traditional stationary infrastructure. We conducted extensive simulation study to assess the effectiveness of AMMNET.

The results confirm that the proposed distributed topology adaptation scheme based on autonomous mobile mesh routers is almost as Effective as a hypothetical centralized technique with complete knowledge of the locations of the mobile clients.The simulation results also indicate that AMMNET is scalable with the number of users. The required number of mobile mesh nodes does not increase with increases in the user population. Although an excessively large number of user groups may affect the performance of AMMNET, the number of user groups is typically very small relative to the number of users for most applications and AMMNET is effective for most practical scenarios.

IX. REFERENCES

[1]. Wei-Liang Shen, Chung-Shiuan Chen Kate Ching-Ju Lin, Member, IEEE, and Kien A. Hua, Fellow,’’Autonomous mobile mesh network’’,IEEE Transaction on mobile computing, 2014.

[2]. A. Petkova, K.A. Hua, and S. Koompairojn, “Processing Approximate Rank Queries in a Wireless Mobile Sensor Environment,” Proc. 11th Int’l Conf. Mobile Data Management (MDM), 2010.

[3]. “Quadrocopter LLC,” http://quadrocopter.us/, 2013.

[4]. R. Roy, Handbook of Mobility Models and Mobile Ad Hoc Networks. Springer, 2010.
[5]. Y.-C. Chen, E. Rosensweig, J. Kurose, and D. Towsley, “Group Detection in Mobility Traces,” Proc. Sixth Int’l Wireless Comm and Mobile Computing Conf. (IWCMC ’10), 2010.
[6]. T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Comm. and Mobile Computing, vol. 2, no. 5, pp. 483-502, 2002.
[7]. X. Hong, M. Gerla, G. Pei, and C. Chiang, “A Group Mobility Model for Ad Hoc Wireless Networks,” Proc. Second ACM Int’l Workshop Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM ’99), 1999.
[8]. K. Blakely and B. Lowekamp, “A Structured Group Mobility Model for the Simulation of Mobile Ad Hoc Networks,” Proc.Second Int’l Workshop Mobility Management & Wireless Access Protocols (MobiWac), 2004.
[9]. Y. Zhang and Y. Fang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks,” IEEE J. Selected Areas in Comm., vol.24, no. 10, pp. 1916-1928, Oct. 2006.
[10]. J. Sun, C. Zhang, and Y. Fang, “A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,” Proc. IEEE INFOCOM, 2008
[11]. B. Salem and J. Hubaux, “Securing Wireless Mesh Networks,” IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.
[12]. R. Gandhi, S. Khuller, and A. Srinivasan, “Approximation Algorithms for Partial Covering Problems,” Proc. 28th Int’l Colloquium Automata, Languages and Programming, pp. 225-236,2001.
[13]. “The Network Simulator - ns-2,” http://www.isi.edu/nsnam/ns, 2013.
[14]. I.F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” Computer Networks, vol. 47, no. 4, pp. 445-487, 2005.
[15]. R. Draves, J. Padhye, and B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks,” Proc. ACM SIGCOMM,2004.
[16]. K.N. Ramachandran, E.M. Belding, K.C. Almeroth, and M.M. Buddhikot, “Interference-Aware Channel Assignment in Multi- Radio Wireless Mesh Networks,” Proc. IEEE INFOCOM, 2006.
[17]. J. Tang, G. Xue, and W. Zhang, “Interference-Aware Topology Control and QoS Routing in Multi-Channel Wireless Mesh Networks,”Proc.ACM MobiHoc, 2005.
[18]. A. Naveed, S. Kanhere, and S. Jha, “Topology Control and Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks,” Proc. IEEE Int’l Conf. Mobile Adhoc and Sensor Systems (MASS), 2007.
[19]. S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, “Coverage Problems in Wireless Ad-Hoc Sensor Networks,”Proc. IEEE INFOCOM, 2001.
[20]. C.-F. Huang and Y.-C. Tseng, “The Coverage Problem in a Wireless Sensor Network,” Mobile Networks and Applications, vol. 10, pp. 519-528, Aug. 2005.