Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 2 – No.2, June 2015 – www.caeaccess.org

Ad-hoc Sensor Networks Issues: Coverage, Protocol and Security

Aiman J. Albarakati
Department of Computer Engineering,
College of Computer and Information Science,
Majmaah University,
Majmaah, Saudi Arabia

ABSTRACT
A mobile ad hoc network (MANET) is an incessantly self-configuring, infrastructure-less network of mobile devices allied without wires. Ad hoc is Latin word and means "for this purpose". (WSN) Wireless Sensor networks have all the indispensable features of ad hoc networks but to unusual degrees e.g. much inferior mobility and much extra inflexible energy necessities. In this article we scrutinize the contemporary status of research and weigh up open problems or challenges in maturity of routing techniques in WSN's.

Keywords
WSN's, MANETs, Routing issues

1. INTRODUCTION
Mull over a wireless network that is made up of entities that act upon both communications and measurements or dimensions. These entities/units are absolutely sovereign and are well competent of copying data from sensors. These entities/units have very low but their data forwarding approach is stout sufficient to be blunder or fault forbearing and to consent to sporadic mobility amongst entities. E.g. we reflect on the sensor network being progressed for the UH Manoa Pods project [9]. The foremost prospects of this concern project is to put into practice a kind of sensor network which is solely to be exploited to cram scarce plants such as ''Silene Hawaiiensis'', just because to dig out that what is indispensable for the plant's endurance in its inhabitant. Here the defy is to put into service an ad hoc network embraced of hundreds of miniature pods or sensors, that will keep an eye on temperature, wind, light, rain and moisture, and which are also utilized for finding out chronological or spatial patterns in the surroundings of the concern plant being premeditated or scrutinized. Such stupendous real life sensor network is encompassing of many sensors. The nodes run on batteries, so here we have networking defy is receiving data back with negligible energy outflow by opting energy proficient paths and in addition with diminishing the routing overhead. Another confrontation or defy is to uphold connectivity in a scenario where some pods are intentionally or Unintentionally shifted to a different or an unusual location or fall short to take part just because of power, even if by and large mobility is expected to be more restricted than in a laptops network. Next issue is that sensor networks can be projected to grow up to countless nodes, so that in these networks any algorithms brought into action and which ought to be scalable. Last but not least, multiple paths should be employed (if applicable) by these networks, for the cause of distributing the energy outflow of forwarding packets and redundancy. The PODS network is likely to be intended to have manifold base stations. Into the bargain, there are no communication constraints in sending data to base stations: dealings between individual sensor nodes may possibly be desirable to allocate distributed computation amid nodes in close geographic immediacy to hold up sporadic communication from the base stations to the individual nodes and also for a multiplicity motives together with fault-tolerance. A lot of research has been carried out in wireless routing protocols. On hand protocols afford unlike tradeoffs amid the subsequent enviable distinctiveness, "distributed computation, fault tolerance, scalability, robustness, and reliability. Current and projected Wireless protocols so far for wireless sensor networks are very restricted; by and large center of attention is communication to a solitary base station or on integration sensor data. Whereas these protocols are appropriate for their anticipated rationale. In this article we see the sights in the utilization of protocols crafted for MANETs to endow with additional all-purpose communication surrounded by nodes in a sensor network, coverage and security concerns.

2. RESEARCH ISSUES
2.1. Design and Coverage Issues
Sensors have outlay/cost, size and weight, limitations, which influence resource accessibility. They have obliged battery resources and obliged processing and communication limits. As supplanting the battery is not conceivable in various applications, low power usage is a fundamental component to be considered, not simply in the hardware and building design, also in the design of algorithms and protocols for networks at all layers of the network structural design. Consequently boosting the lifetime of network is a vital objective. Utilziing a base number of sensors is another clear target, especially in a deterministic node employment practice. A sensor node's radio can be in one of the going hand in hand with four states: transmit, receive, sit out of apparatus/idle, or rest/sleep. The idle state is the time when the transceiver is neither transmitting nor receiving, and the rest/sleep mode is the time when the radio is turned off. As depicted in [37], an examination of the power use for WINS Rockwell seismic sensor shows power use for the transmit state some place around 0.38 and 0.7 W, for receive state 0.36, for the idle state 0.34 W and for the rest express 0.03 W. The power consumed for the distinguishing task is 0.02 W. A charming discernment is that the receive and idle modes may perhaps call for as much energy as transmitting, while in the customary unrehearsed ad-hoc networks,

transmitting may bring into play as high as twofold the power of receiving. Another recognition is the correspondence/computation power usage extent, which can be higher than 1000, thus adjacent/local data planning, data fusion and data compression are significantly charming. Admirably selecting the state of each sensor node's radio is refined through a scheduling approach. This constitutes a key technique for reducing the usage of network energy when the goal is to reduction the number of element sensors performing the degree task. Sometimes, the scheduling approach furthermore has the objective of keeping up coordination among active sensors. The coverage algorithms anticipated are either bound together/centralized on the other hand passed on (distributed). In distributed, the decision strategy or process is decentralized. By appropriated and limited estimations, we suggest an appropriated decision system at each node that makes use of just neighborhood information, within a constant number of hops. Since the ad-hoc sensor networks has a dynamic topology and needs to oblige incalculable, the protocols and algorithms arranged should be appropriated and confined, with a particular deciding objective to better oblige a versatile structural design. The most discussed coverage issues in literature can be requested in the going hand in hand with sorts: area coverage, point coverage and barrier coverage. In light of the subject to be secured particular issues can be itemized considering the going with choices of design:

- *Approach of Sensor exploitation:* deterministic versus unpredictable/random: --- A deterministic sensor course of action may be conceivable neighborly and open situations. Random sensor distribution is for the most part considered in remote or aloof ranges, or for military applications.
- *Range of Sensing and communication:* Ad-hoc sensor networks situations consider sensor nodes with same or diverse detecting ranges. Another element that identifies with network is correspondence or communications extend/range, that can be parallel or not equivalent to the detecting extent.
- *Extra basic necessities:* energy proficiency and connectivity.
- *Algorithm facets:* centralized vs. distributed.
- *Problem Scope/objective:* coverage, greatest network lifetime or undersized sensors.

2.2. Slight Utilization of Energy

MANETs Protocols are solely planned and developed just for communication amongst laptops. Nevertheless laptops are battery powered; their power finances far-off surpass that of a node in a WSN. And such nodes are frequently set up in distant locations. Whether powered by solar energy, batteries or several other ways, dipping energy utilization diminishes the mass or pulls out the life span of the package and constructs the sensor much easier to obscure. Every node in a WSN merely requires to witness, put on the air, and advance data, nothing like a laptop which might possibly have to execute a great deal of multifarious responsibilities. Subsequently, the sensor node computational engine drastically put away not as much of energy than a laptop, and similarly communications exercise a lesser amount of energy. A lot of routing schemes have been planned or crafted for both WSN's and MANETs [3][11][7][12][18][21][22][26][27][28], together with protocols that spotlight on "least energy" routing [21][23][24][25][27][29]. E.g. [23] interprets that a route with shorter hops habitually entails not as much of total energy than a route utilizing fewer but longer hops. Other articles spotlight the development of widespread power aware/energy aware routing methods, scheming power aware cost metrics [23], by means of hand on power regulation to have power over the network topology [19] or via the position information to curtail the power dispatch route, hence diminishing the entire energy utilization [24]. On the other hand not any of these researches focus on realistic issues/defies e.g. overhead of computing such minimum-energy routes. [21] List the subsequent motives why bare minimum energy routing is rigid to put into practice. Least amount energy routing brings in an overhead outlay; the supplementary routing information is not free. Present protocols fall short to endow with satisfactory information for crafting power level pronouncements, inferior power routes abscond not as much of outskirts for channel variations or measurement blunders. Least amount energy routes are thorny to determine and uphold as well. Because of these concerns it is not at present obvious that such "minimum energy" routing is in practice any superior than other schemes which have minor hypothetical competence but endow with other realistic compensations. Just because of these precincts/restrictions we mull over an assortment of protocols declare to make use of negligible energy. [2][5][20][25][28][29] Utilized location information in various MANET protocols both to perk up scalability and to diminish energy utilization [14] [27] [29]. [29] Dig out that a most favorable geographic route may possibly offer power savings and network life span expansion contrast to akin route that doesn't utilize location information. On the other hand this has only been tested for the GEAR protocol beneath a very restricted number of moderately constructive network configurations. [27] Puts forward a clustering based protocol that make use of randomized rotation of confined cluster heads to consistently dispense energy stack/load amongst the sensors. Each local cluster head carry out ''local data fusion'' to pack together the information. It is a solitary path routing method whose scalability is afforded by its hierarchical temperament. Nevertheless, several of their postulations may perhaps not be factual when measure up to general sensor networks e.g. PODS. [29] Endowed with a substitute to this by integrating the method of data diffusion and make use of geographic computations to hit upon small energy paths. They recommended that if the target is fairly far-flung from the packet then the path originated by geographic routing may possibly be virtually as energy competent as a best possible route. [21] Illustrated primarily discovered path that is making use of location information may possibly not be the best energy resourceful path.

2.3. Squat Mobility

MANETs are distinct from Sensor networks by means of mobility. The partaking laptops can moreover be immobile or stir erratically with an indiscriminate pace in MANET. As nodes surrounded by a MANET are in motion, they stir out of range of their neighbors and consequently are no longer capable to commune with the previous neighboring nodes and approach within range of novel nodes. For this reason the mobility brings in the dilemma of fault tolerance. The MANET idyllic routing protocol is supposed to be intelligent to distribute data packets from source to destination even

when some of the transitional nodes stir away from their neighbor's assortment. This makes the routing protocol design obscure as this initiates extra routing overhead. [17] Associated the pace of the movement of the nodes to routing overhead and the packet deliverance ratio. The packet deliverance fraction/ratio deteriorates as speed/pace is greater than before for DSR [8]. While [6] doesn't humiliate as swiftly when mobility boost. In a sensor network nodes are mostly on a static state and with a sporadic infringement of a link as the node displaced or jogs out of its energy. Sensor networks could do with the aptitude to re-configure routinely in a case links fade away or fresh nodes emerge. Protocols like LEACH & GEAR take for granted that the nodes in a sensor network are inert where as on the other hand in PODS as a minimum a number of nodes may possibly be mobile.

2.4. Temperament of self configuration

Ad-hoc WSN's have self-configuring temperament/nature. And which is so called an additional aspect to the vacant ad-hoc temperament of the network. The network is malleable to the shifting necessities and is competent to make out when a sensor node/link fall a short and when it rise up. To design WSN there are two focal approaches, one is the data centric approach and the second one is an address centric approach. A number of routing protocols has been utilized the address centric approach/scheme e.g. GSPR, LAR and DREAM etc. In this approach we allocate IP addresses to all sensor nodes, abridging the progression of routing. This notion is akin to that of standard wired networks. A distinctive IP address will lend a hand the source sensor node to make out the sensor node to which data must be routed. [5] Endowed with an innovative idea of non-address oriented data centric mode. These networks are dissimilar from those of the address centric scheme/approach by means of the method and objective of self-configuration.

2.5. Multipath sought-after

[13] Scheduled qualitative and quantitative self-determining metrics for reviewing the performance/recital of routing protocols of mobile ad-hoc networks. This was a path tactic for one of these qualitative metrics/dimensions. And we have a number of unusual path strategies/approaches. Shortest path strategy [2, 8, 21, 28] is very frequent in which single copy of the message is in the network at any time. [10, 20] Flooding based approach where the message is flooded/inundated all the way through the entire network area. A fine illustration of this approach is the [10] Multi-path On-demand Routing (MOR) Protocol which is a on-demand, load balancing routing protocol intended for the University of Hawaii at Manoa PODS project. MOR may perhaps entail as minute as one network deluge to institute obligatory routes and its energy proficient and vigorous in squat/low mobility and low energy e.g. PODS. Dissemination by and large cracks the routing in extremely mobile state of affairs but bearing in mind our prerequisite for a all-purpose sensor network this is detrimental. The conciliation involving these two approaches is a multipath stratagem, where data packets are routed in the course of a small number of discrete paths and succeeding packets tag along diverse paths at any time doable. This not merely endows with stoutness to the network utilizing multiple paths but also lends a hand in allocation of the energy obligation of the network uniformly athwart the network. [1] Confirm that making use of multiple paths in DSR is capable of carrying on acceptable end to end connections, but they didn't revise the performance/recital perfection on network load balancing. [16] Illustrate that multipath routing know how to balance loads by putting forward a miscellany injection technique to hit upon additional node-disjoint paths weigh against DSR. Nonetheless, their efforts are contention free multiple channel networks based. But they may perhaps not be accessible in several applications. [14] Apply the multipath strategy/approach to DSR's source routing practice and pulls off some scalability under mobile circumstances. Nevertheless the energy allocation constituent of the multipath strategy/approach has not been satisfactorily investigated in the article.

2.6. Ascendibility/scalability

A MANET idyllic routing protocol ought to be ascendible or scalable. It means that whenever the size of the network or the number of nodes increase so the routing protocols must be competent to adapt the changes and endow with best performance based on the provide dimensions. [2] Depicts three schemes, which have been brought into play to grant scalability to a routing protocol for MANETs by the researchers. Opening scheme make use of hierarchy to endow with scalability. Second technique to endow with scalability is caching. The third and final technique to make available scalability is employing geographic information. Utilizing hierarchy to offer scalability is the most commonly exercised practice to level routing as the number of destinations raises. Two most important tactics utilized to coalesce hierarchical network structures and nodes location are the Dominating Set Routing (DSR) and Zone Based Routing (ZBR). [28] Schemes are example of ZBR and GRID is an illustration of DSR. Caching is becoming a far and wide organized practice for the scaling of ad-hoc routing protocols in MANET [6, 8]. This practice trims down the load of routing protocols message in two ways: First It stays away from pushing or approaching topological information where the forwarding load doesn't have need of it and it habitually diminishes the number of hops among the router that has topological information and the router that entails it. [21] Confirmed with their achievement of DSR (energy aware) protocol utilizing mature routes from the cache doesn't unavoidably imply that a low energy route is chosen every time. The final and most commonly utilized practice for endowing scalability to ad-hoc routing protocols is to make use of the geographic location information. This practice takes for granted that all wireless nodes be acquainted with their locations and their links are bi-directional. GPSR and GEAR has been acclimatized this method in gradient routing. For a common sensor network a blend of the aforementioned tactics would be ample to offer scalability.

2.7. Security Risks

A wireless ad-hoc delegated sensor network comprises different sensors spread over a region. Each sensor has remote correspondence limit and some level of information for processing of signal and data networking. A couple examples of remote ad-hoc sensor networks are the going with [29]:

- Military sensor networks to perceive and get however much information as could be normal about enemy advancements, impacts, and other phenomena of side interest [35].

- Sensor networks to perceive and portray natural, biological, chemical, radiological, and dangerous material.
- Make out and screen biological changes in fields, forests, oceans, et cetera.
- Wireless traffic sensor frameworks to keep an eye on vehicle action on roadways or in congested parts of a city.
- Wireless observation sensor networks for giving security in shopping malls, parking and distinctive workplaces.
- Wireless parking lot sensor frameworks to make sense of which spots are occupied and which are free.

Sensor networks computing stances issues to networking in light of the way that the changing physical zone obliges constant reconfiguration of the data links. In case connectivity can't be constantly kept up it moreover obliges applications to handle connected detached from the off-line periods. The code in sensor network nodes overall continues running in untrusted environment. Running code in untrusted environment suggests that programs or its parts are executed on PCs that could have different interests than an inventor of the code. Such tasks are also called mobile code. Mobile code then again, encounters far reaching security issues. From the security motivation behind view there is different risks for the sensor network. Crucial risks take in:

- Communication eavesdropping is the vital strike. The attacker can close from listened or eavesdrop in messages all available information about the sensor network, comprising security vital information and individual nodes position.
- Messages replay is general strike if the assailant is not prepared to break the cryptographic protection of messages however has the limit re-send in advance sent veritable messages.
- Communication disturbance by imbuing noise in the radio channel is a direct strike that can be brought into play to make the correspondence or communication within the network unfathomable. This strike could be made more troublesome by utilizing spread extent radio channels.
- Masquerading the sensor network nodes infers that the attacker conveys its own network node and tries to interface this false node to on hand network.
- Messing about with the node PC infers that the attacker has the limit to make use of direct logical then again physical control with the node to change the behavior of the node and, consequently perform further attacks on the straggling leftovers of the network. The attacker moreover can endeavor to get the cryptographic keys secure in the computer nodes.

2.7.1 Feasible countermeasures

The security countermeasures fall into three zones i) radio channel protection, ii) messages protection, iii) node hardware.

2.7.1.1. Spread Spectrum (SS)

Crucial countermeasure against listening in (Eavesdropping), replay, and irritating is gathered as method of spread spectrum. This countermeasure is as often as possible executed as an approach of frequency hopping. This procedure quickly changes the radio frequency in the midst of data transmission to make attack on the live communication more troublesome. The frequency hopping also constructs the network nodes localization more troublesome and thusly minimizes the danger of uncovering node position.

2.7.1.2. Cryptographic security

The cryptography part is crucial in the design of sensor frameworks/networks that should work in opposing environment with unmistakable threats. The exercise of cryptographic segments can lend a hand to fulfill objectives, for instance, privacy, data uprightness, approval, and non-repudiation. The cryptographic networks brought into play as a piece of sensor network systems fuse secret key encryption and decryption, one-way hash functions, challenge-response cryptographic protocols, and digital signatures. Privacy is ordinarily fulfilled by using secret key encryption methods. Disregarding the way that it can moreover be done by applying asymmetric algorithms, the execution and worth good circumstances of the symmetric counts are all around favored. Integrity of data and affirmation are refined by applying definitely comprehended hashing and MAC algorithms, for instance, SHA and CBC-MAC.

2.7.1.3. Tamper resistant hardware function

The thought of hardware is immovably coupled with the thought of reference monitor/screen. The reference monitor was described in [30] and was standardized in [31]. The reference monitor thought was found to be a key segment of any structure that would give multilevel secure computing workplaces and controls. Reference monitor is furthermore a heart of the huge part of cryptographic modules utilizing secret-key cryptography. A normal execution of reference monitor is a reference acknowledgement part or validation mechanism. Reference acknowledgement part as an execution of the reference monitor thought that acknowledges each reference to data or activities by any customer (program) against a summary of endorsed sorts of reference for that customer." Three blueprint necessities that must be met by a reference acknowledgement part (validation mechanism) are:

1. It must be tamper Proof.
2. It ought to reliably be summoned.
3. It must be adequately little to be subject to examination besides, tests, the satisfaction of which can be ensured.

The utilization of this thought or conception in portrayed structure is done by utilizing the safe microcontroller as a computing subsystem. The utilized microcontroller should constantly have such logical and physical properties that it agrees to the three above conditions. The conditions are met in taking after ways:

1. It is tamper proof because of physical properties of the employed microcontroller, which is made as secure hardware that is safe against physical, electrical, electro-magnetic, and tampering of chemicals.

2. It is summoned because of communication protocols that are the most ideal approaches to compare with the microcontroller.

3. It is adequately little to be obligated to examination and tests, as an aftereffect of smoothness and standardization of the communication protocols that is brought into plays.

For the long time the change resistance of security PCs was recognized without examination. It was known, those broad associations, as Intel then again IBM, can viably make sense of complex chips, however everybody suspected that this kind of attack is far past limits of general aggressors. The issue of surveying the level of change resistance offered by a given thing has been overlooked by the security research bunch. It was discovered already that strikes on change resistance are possible in like manner by undersized associations and even by individuals (see [9]). The tamper resistance of smartcards and security processors must be right away about investigated thing by thing to discover possible vulnerabilities or weakness.

2.7.1.4. The model of Communication system

The utilized communication model system is delineated with the desire of proliferation of diverse attacks and security against these strikes. Generally the sensor networks nodes bring into play communication of radio frequency, so broadcast is the vital communication primitive. This primitive is not to a great degree suitable for message routing; so on this primitive is amassed a communication primitive bringing into play bidirectional links. This model has similarly another purpose of inclination – it allows utilizing business off-the-shelf radio correspondence modules, for instance, Bluetooth or WiFi that reinforce the bidirectional associations/links. Yet communication standards of both WiFi and Bluetooth hold up cryptographic security of transmitted messages, this facet is not brought into play as a piece of sensor networks. The security instruments of these standards support only security of transmission between two nodes, however not the security of messages traded through number of nodes, that could be possibly untrusted. The security of transmitted data is given on the packet level for the reason that of dynamic routing. All packets are cryptographically guaranteed by symmetric Secret-key, shared between sending and receiving nodes. The key is secure in tamper resistant hardware. These shared keys licenses shared approval/authentication of passing on nodes. Security and uprightness is given by symmetric encryption. All packets are encoded utilizing secret key and symmetric cipher, shared between sending and receiving node.

3. CONCLUSION

This research article was all about evaluation of the indispensable aspects of the routing protocols for all-purpose WSN like [9]. Contemporary research for MANETs routing protocols and ad-hoc sensor networks have a propensity to construct numerous tradeoffs in a variety of aspects and are usually experienced in a much synchronized setting. The requirements and necessities of general ad hoc sensor networks routing protocols are very distinctive compared to MANETs routing protocols and other sensor networks. Sensor networks can possibly give vital advantages to information assembling in threatening environment if actualized with proper security. These systems can't be made completely secure against a wide range of assault. Deciding the suitable level of security for a specific framework/system/network ought to include thought of the greatness of potential dangers, the expense/cost of actualizing fluctuating levels of security and the effect on the usefulness or functionality of the entirety network. The portrayed undertaking is in this time in the period of the outlining and testing different segments of the system utilizing diverse methodologies. For this reason we can say that there is a call for more scrutiny and study into this innovative field as it constitutes several of its inimitable defies.

4. REFERENCES

[1] “Das and Nasipuri ”, ‘’On demand Multipath Routing for Mobile Ad Hoc Network’’, (IC3N), 8th International Conference on Computer Communications and Networks Boston, 1999

[2] “Kung and Karp ”, ‘’ Greedy peimeter stateless routing for wireless networks(GPSR)’’, MOBICOM, August 2000.

[3] “Krishnamachari”, ‘’Modeling Data-Centric Routing in Wireless sensor networks’’

[4] “C.E.Jones et al.”,’’A Survey of energy efficient network protocols for wireless networks’’

[5] “Chalermek, Estrin and Govindan”, ‘’Directed Diffusion: A scalable and robust communication paradigm for sensor networks’’, ACM MOBICOMM, Boston, MA, 2000

[6] “Royer and Perkins”, ‘’Ad hoc on demand distance vector routing’’, 2nd IEEE Workshop on Mobile Computer System and Applications, February 1999.

[7] “Govindan, Estrin and Kumar, Heidemann”, ‘’Next century challenges: Scalable co-ordination in sensor networks’’, MOBICOM, 1999, Seattle.

[8] “Maltz and Johnson”, ‘’Dynamic source routing in ad hoc wireless networks’’, Mobile computing, Chapter 5, Luwer Academic Publishers, 1996.

[9] “Biagioni, Chee ,Bridges”, ‘’PODS: A remote ecological Micro sensor network ‘’, http://www.botany.hawaii.edu/pods/overview.htm

[10]” Bridges and Biagioni”, ‘’The Application of Remote Sensor Technology to Assist the Recovery of Rare and Endangered Species’’, International Journal of High Performance Computing Applications, Vol. 16, N. 3 (August 2002).

[11] “Aron.”, ‘’On the scalability of on-demand routing protocols for mobile ad hoc networks: an analytical study’’

[12] “Xu and Stojmenovic”, ‘’Power-aware localized routing in wireless networks’’, IEEE Int. Parallel and distributed processing symp., Cancun, Mexico, May 1-5, 2000,

[13] “Corson and Macker ”, ‘’Mobile ad-hoc networking and the IETF’’, Mobile computing and communications review, 2, 1, 1998, 9-14.

[14] “Harms and Wu”, ‘’On-demand multipath routing for mobile ad-hoc networks’’, Computer science department, University of Alberta, AB, Canada.

[15] ” Widmer and Mauve”, ‘’A Survey on Position-Based Routing in Mobile Ad Hoc Networks’’.

[16] “Sholander, Perlman, Hass and Tabrizi”, ‘’On the impact of Alternate Path Routing for load balancing in Mobile Ad Hoc Networks’’, IEEE/ACM MobiHoc 2000, Boston, 2000

[17] “Kongmunvattana and Nagar”, ‘’Analysis of Routing Protocol Performance on Multi-Hop Wireless Ad Hoc Networks’’, International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'2001), Las Vegas, June 25-28, 2001

[18] “ Robert D”, ‘’Gradient Routing in Ad Hoc Networks’’

[19] “Rosales-hain and Ramanathan ”, ‘’Topology control of multi-hop wireless networks using transmit power adjustment’’, IEEE INFOCOM 2000, pp. 404-413.

[20] “Chtamtac, Syrotiuk, Basagni and Woodward”, ‘’A distance routing effect algorithm for mobility (DREAM)’’, MOBICOM, 1998, 76-84.

[21] “Brown and Doshi”, ‘’Minimum energy routing schemes for a wireless ad hoc network’’, IEEE INFOCOM 2002.

[22] “Giordano and Stojmenovic et al.”,’’Position based Routing: Algorithms for Ad Hoc Networks: ATaxonomy’’

[23] “Singh, M. and Raghavendra”, ‘’Power aware routing in mobile ad-hoc networks’’, MOBICOM, 1998, pp. 181-190.

[24] “Ruduplu and Meng”, ‘’Minimum energy mobile wireless networks’’, IEEE JSAC, v.17, n.8, August 1999, pp. 13333-44.

[25] “Tseng, Liao and Sheu”, ‘’GRID: A fully location-aware routing protocols for mobile ad-hoc networks’’, IEEE HICSS, January 2000.

[26] “Heinzelman, Chandrakasan and Balakrishnan”, “Energy efficient routing protocols for wireless microsensor networks’’, HICSS, Hawaii, January 2000.

[27] “Heinzelman, Chandrakasan, Rabiner and Balakrishnan”, ‘’Energy-efficient communication protocol for wireless microsensor networks’’, 33rd HICSS, 2000

[28] “Vaidhya and Ko”, ‘’Location-aided routing (LAR) in mobile ad hoc networks’’, MOBICOM, 1998, pp. 66-75.

[29] NIST, Advanced Networks Technologies Division, http://w3.antd.nist.gov/wahn_ssn.shtml

[30] Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I,

ESD/AFSC, Hanscom AFB, Bedford, Mass.

[31] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28.

[32] Anderson, R.J., Kuhn, M.: Tamper Resistance - a Cautionary Note, in The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California,

[33] Wensheng Zhang, G Cao and Tom La Porta,”Data Dissemination with Ring Based Index for Wireless Sensor Networks”, IEEE Transactions on mobile computing, Vol 6, No 7, July 2007.

[34] Ryo Sugihara and Rajesh K.Gupta,”Programming Models for SensorNetworks: A Survey”, ACM Transactions on sensor networks 2006.

[35] Ajit Warrier et.al, “Mitigating Starvation in Wireless Sensor Networks”, Military Communications Conference, 2006, MILCOm 2006, pp 1-5.

[36] S.Duan and Xiaobu Yuan,”Exploring Hierarchy Architecture for Wireless Sensor Network Management”, IEEE 2006.

[37] V. Raghunathan, C. Schurgers, S. Park, M.B. Srivastava, Energyaware wireless microsensor networks, IEEE Signal Processing Magazine 19 (2002) 40–50.