iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4120

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Geographical Routing Protocols in Wireless Sensor Networks

Syeda Gauhar Fatima[1], Syeda Kausar Fatima[2], Abeer Arif [3]
[1]*Professor ECE dept, Deccan College of Engineering and Technology, Darussalam, Hyderebad.*
[2]*Research Scholar ECE dept. , JNTUH, Kukatpally, Hyderabad*
[3]*Students ECE dept, Deccan College of Engineering and Technology, Darussalam, Hyderabad.*

Abstract: Wireless sensor networks offer inexpensive solutions in a wide variety of applications ranging from health, home, roads and public area monitoring to industry and aircraft control. As sensors proliferate, scalable communication protocols with low implementation requirements are pursued. Another key issue for deployment of these solutions is security since the wireless sensor networks themselves are prone to security attacks. In this paper, we review geographical routing protocols, which allow for high scalability due to their localized operation while they also support mobility consuming less node and network resources since they operate on very limited overhead. We also investigate their vulnerabilities to security attacks and report efficient counter measures.

Keywords: Component, Sensor networks, routing protocol, security, scalability, geographical routing, routing attacks.

I. INTRODUCTION

Routing in wireless sensor networks is performed in a cooperative way, i.e. each node relies on its neighbors to forward its packets towards the network sink. In other words, all sensor nodes participate in the routing procedure acting as routers. This intricacy of the sensor networks implies that the routing functionality is distributed over all network nodes, which however have limited energy, memory and processing capabilities. For this reason, traditional routing protocols are not applicable and new ones have been designed. In this infrastructure-less environment, the detection of (the ad hoc) topology is a key component of the routing which additionally has to support mobility. Moreover, it soon became apparent that efficient support of scalability is required, since a) redundancy is of primary importance for undisturbed sensor network operation and b) the sensor population grows very rapidly. As regards efficiency, this is expressed in terms of successful packet delivery ratios, as well as low (routing) overhead since this affects the consumed bandwidth, power, processing and memory resources which in turn defines the network's lifetime. Although a plethora of routing protocols for ad hoc and sensor networks has been proposed, geographical routing (GR) targets the efficient support of mobility and scalability while it turns out to be invulnerable against a set of security attacks when security comes into play. While hierarchy and node clustering have also been proposed to address the scalability problem, GR outperforms other solutions because it addresses at the same time scalability and mobility. The concept is to use geography for routing instead of measuring hops and flooding the current state of all network nodes to create a map. In more detail, the idea is that each node is characterized by its coordinates and each time a node needs to send a packet, it will forward it to the neighbouring node that is closer to the destination than all the rest nodes. To perform this decision, it is required to keep geographical information (the location) for each neighbour in its routing table. This information is gathered through the so-called "BEACON" messages that each node periodically transmits announcing its location, although geographical routing protocols obviating this location information have also been proposed. This localized operation has the following important advantages:

1) It facilitates the mobility support. Since each node beacons its coordinates periodically, all its neighbours update their routing tables accordingly. Thus, each node is aware of its alive neighbours at any time, refreshing their location when BEACON messages are received and deleting nodes when they stop sending BEACON messages.

2) It is scalable. The routing protocol interactions as well as the routing table dimensions do not depend on the size of the sensor network. The BEACON messages are transmitted periodically, irrespective of the number of nodes in the network while the size of the routing table depends only on the number of nodes in the neighborhood, i.e. on the network density and not the network population. This way wide sensor networks consisting of thousands of nodes can be realized without any need for cluster formation, which introduces complexity.

3) It introduces minimal routing overhead. Since all nodes are only interested in knowing their neighbours locations, there is no other need for information exchange. This way no routing message is propagating through the network, and only localized

interactions take place. This way bandwidth is economized, processing and transmission energy is saved and routing table dimensions decrease, thus representing an attractive approach for routing in WSNs.

GR is a proactive routing protocol since beacons are emitted periodically. The disadvantage of proactive routing protocols is that routing messages are exchanged even when no traffic to route exists. This is alleviated adopting a piggybacking approach: in each transmitted packet, the source adds its coordinates, and all nodes are in promiscuous mode, thus listening the coordinates of their neighbours even when they are not sending a beacon but a data packet. This way, the inter-beacon timer is refreshed with every packet transmission.

The realization of GR algorithms requires that each node is aware of its coordinates either due to the existence of a GPS (Global Positioning System) device in each sensor node or based on the implementation of some localization functionality. This aspect has attracted much attention since it directly affects the cost of the sensor node and the achieved security, as will be detailed later on.

The rest of the paper is organized as follows: first, current trends in routing protocols are briefly discussed (in section II) and then a set of geographical routing algorithms are presented in section III. In section IV solutions addressing the localization problem are reported while in section V, enhancements aiming at higher security are explored. Finally, conclusions are drawn in section VI.

II. CURRENT TRENDS IN ROUTING IN WSNS

Routing protocol design has attracted significant research attention during the last decade. The results include numerous approaches classified using different criteria for example in proactive vs. reactive approaches, in link/path state protocol versus hop by hop routing e.t.c. The last few years, given the proliferation of sensor node application and the dramatic growth of their population, the IETF is currently standardizing the RPL protocol [17][17] which constructs Directed Acyclic Graphs based on a variety of alternative routing metric, which is a link-state protocol. On the other hand, significant effort has been spent on Delay-Tolerant Networking where the associated routing protocols target enhanced reliability for delay-tolerant applications and network coding is also pursued as a means to enhance reliability at the expense of redundant packet transmissions.

In this environment, one could claim that the geographical routing is losing its momentum mainly due to its requirement for location information availability. But this is not the case, because

A. A great variety of applications requires the availability of location information. Once this information is built and maintained it can be exploited for routing purposes as well.
B. Location-based routing protocols that obviate the need for geographical position knowledge have been presented, as will be detailed later on.
C. It outperforms other protocols when scalability and mobility has to be supported.

Among the applications requiring the maintenance of location information, the logistics enterprise control, e-health monitoring applications and vehicle to vehicle information sensing and exchange can be found. These applications are all at the focus of the ICT economy since they affect the industry competitiveness, the human well-being and the fiscal situation in the growing European population and last but not least the transportation safety and efficiency. For these reasons, the authors anticipate that geographical routing will not be passed over in the forthcoming years, since it offers a clear, low cost solution for WSN killer applications.

III. GEOGRAPHICAL ROUTING PROTOCOLS

The most widely cited geographical routing protocol is the Greedy Perimeter Stateless Routing (GPSR) algorithm for wireless sensor networks initially presented by Karp and Kung (2000) in [1][1]. The protocol is shown to choose paths with lower hop count than Dynamic Source Routing protocol (DSR) due to the extensive use of geographical coordinates. It also reduces routing overhead by 30% compared with DSR algorithm when nodes move with a maximum speed of 20m/s due to localized interactions. Moreover, it is shown to increase the achieved throughput when the number of nodes increases above 100, proving the scalability feature of geographical routing. The algorithm consists of two methods for forwarding packets: *greedy forwarding, and perimeter forwarding*. In greedy forwarding, the source node transmits the packet towards the neighbours that is closest to the destination (and furthest from the source node), which is the locally optimal choice of next hop. This implies that each node needs to know only the addresses and coordinates of its immediate neighbours, thus the routing table dimension depends on the density of the network and the radio range of the node and not on the dimensions of the network as a whole. When greedy forwarding is not possible and the packet has not reached its destination, i.e. there is a void between the node and the destination, perimeter forwarding is performed to travel around the void. This is achieved based on the proactive calculation of planar graphs. (The details of the algorithm can be found in the same work, and are outside the scope of our study.)

Further energy consumption-related improvements have been pursued by Yu, Estrin, and Govindan (2001) in [2] where "geographical and energy aware routing" (GEAR) is proposed. In GEAR, the next hop is decided taking into account the value of the learned cost function for each neighbor apart from its location. This "learned cost" function reflects the available (remaining) energy of each node, thus allowing for better load balancing among neighbors. This introduces the need for each node to inform its neighbors about the level of its remaining energy periodically. The efficiency of the algorithm is not significantly affected by the energy reporting frequency (it is not degraded even when this is done infrequently) since each node estimates its neighbors remaining energy between two announcements. This however adds complexity in the sensor node. Another differentiating point is that in this work packets are considered to be destined to a group of nodes located in the same region rather than destined to a single destination node. In this case, once the packet has arrived to one node of the region, the desired nodes can be reached following two different approaches: restricted flooding or recursive geographical forwarding which further reduces the energy consumption. The latter defines that each region can be split in sub-regions in an iterative way so that the packet finally reaches its destinations. Modifying the stopping rules, the algorithm can be used to route packet to single destinations. This approach can be considered as an application of clustering architectures to geographically routed sensor networks. To this end, using computer simulations (in ns2 simulator) GEAR is shown to extend the network lifetime up to 30% compared to GPSR under certain circumstances. Working in the same direction, Haider, Javed, and Khattak (2007) in [14] have evaluated their Energy Aware Greedy Routing (EAGR) protocol which also relies on energy information to prolong the lifetime of the network. In this work, nodes with remaining energy below a predefined threshold are considered as dead and are excluded from the list of candidate for forwarding neighbours.

A combination of geographical information with energy information is also adopted by T. Roosta, M. Menzo, and S. Sastry (2005) in [3], where the Probabilistic Geographic Routing (PGR) protocol is presented. It keeps the concept of localized routing decision followed in all geographical routing protocols and topology changes are traced using beacon messages. The novel approach is the probabilistic forwarding which is performed as follows: in order to forward a packet, the node selects a set of candidate nodes based on geographical information to guarantee that the packet will be forwarded and not travel backwards. These candidate nodes are then assigned a probability proportional to their residual energy and link reliability. Finally the next hop is decided taking into account these probabilities following a simple roulette wheel algorithm. The performance of the algorithm is evaluated using the ns-2 simulation platform and is shown to offer higher throughput and longer system lifetime at the expense of slightly longer paths compared to GPSR.

Energy awareness is adopted by Shuhui Ma and Hong Ji (2006) in [18], where they present a cross-layer energy aware geographical routing protocol named Energy-aware Geographical Forwarding using Adaptive Sleeping (EnGFAS). In EnGFAS, nodes sleep not only to save energy but also to save collisions at the MAC layer. Additionally, to avoid forwarding the fragments of a single application layer packet through different neighbours, the source node calculates whether a neighbour node has enough energy (more than Ethr) to forward the whole application layer packet. This energy threshold (Ethr) is defined based on the value in the 'duration' field of the RTS message of the MAC layer.

Further insight about the combination of directional transmission with randomized location–based routing is provided by Israat Tanzeena Haque, Ioanis Nikolaidis and Pawel Gburzynski (2007) in [14], where such an algorithm called Directional Location-based Randomized Routing (DLR) is presented. This novel approach is compared with PGR and it is shown through computer simulation that while the packet delivery rate increases, such schemes must be carefully designed in order to achieve the desired goals.

A variant of GPSR called On Demand GPSR (OD-GPSR) dealing with asymmetrical links and addressing the data consistency problem is presented in [13]. It also addresses the GPSR inefficiency in identifying the home node when the target location is outside the exterior perimeter of the sensor. In other words, it improves GPSR at the cost of a slight increase in delay performance.

To further enhance mobility support in dense sensor networks, Witt and Turau in [6] have proposed another geographical routing algorithm called Blind Geographic Routing (BGR). Although it uses no topology information, it relies on the implementation of timers in each node which are set depending on their location. This is very useful when the topology changes rapidly or the wireless communication is unreliable. BGR does not rely on topology information but adopts the notion of forwarding areas. Each time a packet has to be forwarded, it is broadcasted to a forwarding area; all nodes in this area calculate a timer based on their distance from the destination. The node whose timer expires first, forwards the packet. The forwarding area must be small enough so that all nodes within it can communicate with each other, and large enough to contain a sufficient number of nodes. Once a node forwards the packet, all other nodes within the forwarding area also receive this packet and know that it has been forwarded, so they cancel their timers.

As greedy routing fails in case of a local minimum, a recovery strategy is needed to guarantee delivery. The preferred recovery method for conventional geographic routing is face routing on a planar subgraph, which is constructed from neighborhood information. But in beaconless routing the full knowledge of the neighborhood is not available beforehand. Instead, part of this knowledge has to be gained by exchanging messages, if it is not implicitly given by the location of the nodes. Techniques to deal with the beaconless recovery problem have been proposed [15] and evaluated in [16]. Geographical information is exploited to elongate the network lifetime though energy conservation following a "geographical adaptive fidelity" (GAF) algorithm presented by Ya Xu, John Heidemann, Deborah Estrin (2001) in [3]. In sensor networks where the energy level maps directly to lifetime, the authors propose to turn off a subset of the sensors based on their area coverage and application i.e. equivalent nodes (two sensors that detect the same event in the same area) are periodically turned off so that one is active each time. Although GAF does not rely on geographical routing, it requires the collection of geographical and energy information in each node. This information can be exploited to perform geographical routing reducing the overall memory requirements. The implementation of GAF achieves lifetime extension by 30-40% while it additionally supports node mobility.

IV. LOCATION INFORMATION

To perform routing based on geographical information requires that each node is aware of its geographical position and accordingly informs its neighbours. Although the straightforward solution is to equip each node with a GPS (Global Positioning System) device, it increases the cost and the size of the sensor node. When this is not required for the application execution, to overcome this drawback, localization algorithms have been designed and implemented. They allow for the calculation of the relative position of nodes using few nodes as anchors. Although these algorithms require the exchange of messages and cooperation among the sensor nodes, which consumes bandwidth and transmission resources, the overall cost is significantly lower than that of the GPS device.

Localisation techniques can be classified in two categories [4]: triangulation and free-range localization. In the first case, few nodes are assumed to know their location and broadcast it to all their one-hop neighbours. Based on three measurements, each node can calculate its own location comparing the signal strength from each neighbour or the time difference of the received messages. Another option is to derive coarse grained location information applying heuristics based on the received beacon messages.

Location inaccuracies in general lead to performance degradation while if location is intentionally falsified (by a malicious node), network collapse may be caused in geographically routed sensor networks. The impact of different distributions of location errors in delivery ratio and hop count for two geographical algorithms (GPSR and BGR) have been investigated and reported in [6]. Due to the important performance deterioration, significant research effort has been put to location verification and techniques to overcome this vulnerability. In [6], modification for GPSR and BGR are proposed while in [5], more radical solutions are presented. In more detail, in [5] , Lin et. al. propose nodes clustering based on geographical information and the selection of cluster head based on location (close to the cluster area center) and energy resources. When nodes move inside their cluster, only the cluster head is notified, minimizing the overall overhead, while routing is performed based on geographical information among clusters. The end result is that Location-fault tolerant Geographical Routing is shown to maintain 75% throughput even in the presence of 15% location inaccuracies while GPSR performance drops in this case below 40% at the cost of cluster set-up procedure.

In an attempt to deal with the localization issue, geographical routing protocols based on "Virtual coordinates" have been presented (e.g. [7], [8]). The assumption in these works is that only two designated nodes are aware of their location and virtual coordinates are calculated based on local connectivity. First, perimeter nodes are identified based on their distance from the two designated bootstrap nodes. Then the perimeter nodes estimate their coordinates and next all other nodes define their coordinates based on the messages sent by the perimeter nodes. To support mobility, this procedure is periodically executed. While in [7] virtual coordinates intend to approximate physical coordinates, in [8], the relevance of data is exploited and data fusion is adopted thus turning virtual coordinates to logical coordinates to improve the overall performance at the expense of intelligence in the nodes.

V. SECURITY ISSUES IN GEOGRAPHICAL ROUTING

Wireless sensor networks are more prone to security attacks than legacy wired communication networks, because wireless media is easily overheard while the limited bandwidth and node capabilities (in terms of power, processing and storage) impedes the adoption of well-known security solutions. A great part of security attacks target the routing protocol driving researchers to pursue techniques for protection. Geographical routing protocols are inherently less vulnerable to routing attacks mainly due to their local (almost stateless) operation. Let us remind here, that in GR each node maintains a list of its one-hop neighbour based on periodically transmitted BEACON messages. Thus, a malicious node that intends to allure traffic either to process it and obtain the included information or just to drop it disrupting the network's operation, should pretend to exist in one or more locations (possibly

all) different from the real one. This type of attack is called “sybil” attack and the respective countermeasures are mainly related to location verification in geographically routed networks. Another attack applicable to all routing protocols including GR is the forwarding attack: a malicious node does not forward any or part of the received packets, decreasing this way the delivery ratio of the sensor network. In the sequence, we report solutions for both types of attacks.

A. Defending Sybil Attack

To prevent Sybil attack, a key management scheme can be adopted. In [9], Hao et. al. report a number of key-based techniques that can be used, stressing however, that the limited processing capabilities of sensor node should be carefully taken into account. For this reason, the authors designed a distributed node verification scheme. The network is organized in clusters based on location information and the cluster head undertakes the responsibility of verifying the identity of the nodes in its cluster based on a proper key management protocol.

Another way to prevent a sensor node from faking its location, is to verify its location challenging it. When the node receives the challenge, it should immediately reply to the verifier, through an ultrasonic channel, with a nonce that was included in the original challenge message. However, this solution requires extra hardware which may increase the cost and the size of the sensor node.

In [4], the authors propose to reverse the triangulation scheme in order to provide secure localization: when node A needs to define its location, it does not calculate it on its own but its neighbors communicate in order to define node’s A position. The geometry and the principle of position calculation is the same but is now performed by more than one nodes, thus making more difficult the realisation of Sybil Attack. To be more precise, nodes are distinguished in plain sensor nodes and anchor nodes. A plain node issues a localisation request and at least three anchor nodes should receive it in order to define its location. This solution is based on the assumption that anchor nodes are trustworthy.

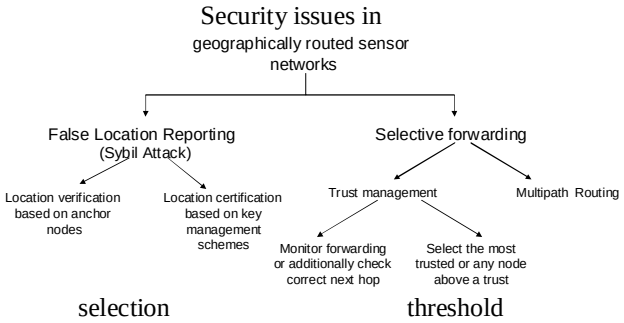


Figure 1. The main security attacks threatening sensor networks based on geographical routing and defense directions

Although the previously described location verification procedure renders the system more robust, it is vulnerable to a set of more sophisticated attacks. For example, a node can cheat by transmitting at a higher or lower power to appear closer or further than it is. This attack can be defeated based on the cooperation of the three anchors. Another attack is to prevent consensus on the location among the anchors while the most difficult to defend attack is “mobility”, i.e. a node’s location is defined and then the node moves to a different location. Defense against these attack types are discussed in [12]. In general, security in sensor networks follows the same story as security in communication networks and information systems. Each time a new attack type is detected, countermeasures are designed which will break down later on and this keeps going on as long as human brain is thinking out.

B. Defending Selective forwarding attack

In wireless sensor networks, nodes rely on their neighbours cooperation to route their packets towards the base station. The correct execution of the routing protocol is of key importance for the overall network operation. However, a very easily implemented routing attack is selective forwarding or even blackhole attack. In the first, a node drops part of the packets it was assumed to forward while in the second it refuses to forward any received packet. To defend against these attacks, the nodes should be capable of detecting malicious nodes and exclude them from their forwarding candidates list. To detect this behaviour it is necessary that each node checks whether the selected next hop neighbour has forwarded the packet either based on some type of acknowledgement or overhearing its transmissions. This way the trustworthiness of the neighbours can be defined and taken into account during routing decisions. Although numerous trust management schemes for wireless sensor networks can be found in the literature, here we will focus on their applicability in geographical routing protocols and on the achieved security enhancements. In [10], the authors present an enhancement of GPSR where the next hop is decided taking account the trustworthiness of the neighbours apart

from their location. To evaluate the trustworthiness of each neighbour, each time node A selects node B as the next hop, it listens node's B transmission waiting (for a fixed time interval) to listen its own packet correctly forwarded. Based on the outcome of this procedure, two trust metrics are calculated: the first expresses the ratio of forwarded packets while the second expresses whether these have been appropriately (without any modification) forwarded. Each trust component is expressed as follows:

$$T_i^{A,B} = \frac{S_i^{A,B} - F_i^{A,B}}{S_i^{A,B} + F_i^{A,B}}$$

where $S_i^{A,B}$ is the number of successful type i events (forwarding or packet correctness) that A has measured for B, and $F_i^{A,B}$ is the number of failed type i events that A has measured for B. Thus, each metric ranges from -1 to 1 and the overall node trust value is a weighted sum of these two trust components. Finally, when selecting the next hop, the node closest to the destination and with the highest trust value is chosen. This way, malicious nodes are detected and avoided and the packet delivery ratio of plain GPSR is improved by 30% for 50% of adversary nodes. Another variant of GPSR enriched with trust awareness but also energy-awareness to elongate the network's lifetime has been proposed in [11]. In this work, the trust, energy and distance metric are combined in a weighted additive manner, enabling the flexible shift from trust to energy efficiency and latency, depending on the requirements of the application at hand. The proposed ATSR adopts a location-based approach to reduce the routing protocol storage and processing requirements, while it realises a distributed trust model incorporating both direct and indirect trust information. The next hop selection is decided upon a novel routing function which allows for balancing between pure routing and security criteria. The weights introduced in the calculation of the total trust value as well as those introduced in the routing function allow for flexible configuration, trade-offs and fine tuning of the algorithm as shown through computer simulations. The simulation results prove that ATSR successfully reveals malicious nodes even when they represent the 50% of the network nodes and even if they perform different attack types, and defines alternative trusted routes to the destination. The adopted reputation exchange protocol assists nodes in discovering adversaries existing in their neighborhood reaching a delivery ratio of more than 99%. Last but not least, an important advantage of the presented ATSR protocol is that it represents a readily deployable solution. A more sophisticated approach addressing selective forwarding and denial of service attack caused by data flooding at the same time is proposed in [4]. In flooding attack, a malicious or faulty node can send an excessive number of packets to overload the receiving nodes and block packets originating from other sources. This work proposes an interesting combination of a set of measures to design a highly robust routing solution. To deal with flooding attack, each node computes the expected data rate from its neighbours based on data received by the base station querying the sensor nodes. Once the expected rate from each neighbour is defined, excessive packets can either be droped or forwarded with lower priority than those within the defined rate. This implies that strict priority is adopted for routing. Additionally, low priority packet are exploited to collect forwarding evidence and thus detect nodes performing selective forwarding. To evaluate the trustworthiness of its neighbours, each node overhears its neighbours' transmissions to check whether they have forwarded a packet, sincerely executing the routing protocol. Following the approach presented in [4], the low priority packets are not strictly forwarded to the next hop node dictated by the geographical protocol but low priority traffic is spread to a wider list of neighbours so as to evaluate their trustworthiness. If the packet is not forwarded, then a misbehaving node has been detected at the cost of dropping a low priority packet. A side effect of this solution is load balancing. To further enhance security protecting against routing attacks and improve the time required to detect a malicious node, this work suggests that the source node not only overhears its neighbour forwarding the packets (as proposed in other works) but also checks whether the neighbour has appropriately selected the next hop either querying the anchor or keeping in its routing table not only the one hop but also two hop neighbours. Robustness is further enhanced adopting multi-path routing which however consumes network resources. Multi-path routing is also proposed in [9], as a measure of defense against selective forwarding attack. In [4], once the set of candidates next hop nodes is defined based on geographical information, the probability of selecting each node is defined based on trust evidence. K nodes with probability higher than an applicationrelated threshold are selected based on the roulette wheel algorithm. K defines the level of flooding. Although the solution presented in [4] includes a number of novel ideas, it requires the implementation of significant intelligence in the node for the calculation of the expected rate, the priority queuing of the packets and the differentiated routing decisions per priority. It also introduces significant overhead for communication between nodes and anchor for each transmitted packet. To keep up with trust model design, a reputation scheme is also mentioned in [4] but not evaluated. This works as follows: when node A needs to define the trustworthiness of node B, apart from monitoring node B's behaviour, it also asks its neighbours to provide their opinion about node B. These schemes accelerate the malicious behaviour detection process and allow for more secure calculation of the trust values, introducing however the need for message exchange for the communication of trust values.

VI. CONCLUSION

In geographically routed wireless sensor networks, routing is performed on hop-by-hop basis where each hop is decided based on location information of all one-hop away neighbours. This localized operation presents significant advantages which include the support of mobility, the support of high scalability while overhead and node requirements remain minimal. Different algorithms exploiting location information in diverse ways or combining it with remaining energy or sensing coverage area information have been built on the geographical routing principle, proving its value. The location information required to perform geographical routing can be achieved through a variety of techniques at different implementation costs. As regards security, which is of key importance in this environment, geographical routing resists more to adversaries, since to perform Sybil attack, a malicious node has to cheat the localization scheme. Even if it succeeds, it cannot allure traffic, as would happen in other routing protocols, since routing is decided only based on location information. Forwarding attacks can be easily defended, realizing a distributed trust model. To this end, geographical routing can be exploited to build scalable, dense, secure and energy-aware ad hoc wireless sensor networks supporting high mobility levels.

VII. ACKNOWLEDGMENT

The work presented in this paper was partially supported by the GSRT-funded 09ΣΥΝ-52-741 “EXECHON” project.

REFERENCES

[1] Brad Karp, H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for WirelessNetworks”, MobiCom 2000.

[2] Y. Yu, D. Estrin, and R. Govindan. “Geographical and EnergyAware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks”. UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.

[3] T. Roosta, M. Menzo, and S. Sastry. Probabilistic Geographic Routing in Ad Hoc and Sensor Networks” International Workshop on Wireless Ad-hoc Networks, 23-26 May 2005, London, UK.

[4] K.D. Kang, K. Liu, and N. Abu-Ghazaleh “Securing Geographic Routing in Wireless Sensor Networks”, 9th Annual NYS Cyber Security Conference: Symposium on Information Assurance, June 1415, 2006, Albany, New York.

[5] Junlong Lin, Geng-Sheng (G. S.) Kuo, ”A Novel Location-fault-tolerant Geographic Routing Scheme for Wireless Ad Hoc Networks”, Vehicular Technology Conference, 2006, 7-10 May 2006, Melbourne, Australia.

[6] Matthias Witt Volker Turau, “The Impact of Location Errors on Geographic Routing in Sensor Networks”, International Conference on Wireless and Mobile Communications, (ICWMC '06), 29-31 July 2006, Bucharest, Romania.

[7] Ananth Rao, Sylvia Ratnasamy, Christos Papadimitriou, Scott Shenker, and Ion Stoica, “Geographic routing without location information”. In MobiCom, 2003, September 14-19, 2003, San Diego, California.

[8] Bin Yu, Katia Sycara, “Geographic Routing in Distributed Sensor Systems without Location Information”, Proceedings of the Ninth International Conference on Information Fusion (FUSION), 2006, Florence (Italy), 10-13 July 2006.

[9] Wu Hao, Cheng Chao Li, Cheng-shu, “Research on One Kind of Improved GPSR Secure Routing Protocol”, IEEE 2007 International Symposium on Microwave, Antenna, Propagation, and EMC Technologies For Wireless Communications, 14-17 August 2007 Hangzhou, China.

[10] Asad Amir Pirzada and Chris McDonald “Trusted Greedy Perimeter Stateless Routing”, IEEE, ICON2007, 19-21 July 2007, Adelaide, South Australia.

[11] T. Zahariadis, P. Trakadas, H.C. Leligou, S. Maniatis, P. Karkazis, “A novel trust-aware geographical routing scheme for wireless sensor networks”, Wireless Personal Communications, 2012.

[12] Nael AbuGhazaleh, KyoungDon Kang and Ke Liu “Towards Resilient Geographic Routing in WSNs”, MSWiM’05, October 10–13, 2005, Montreal, Quebec, Canada.

[13] Jian Chen Yong Guan Udo Pooch, Customizing GPSR for Wireless Sensor Networks”, 2004 IEEE International Conference on Mobile Adhoc and Sensor Systems, October 24-27, 2004, Fort Lauderdale, Florida, USA .

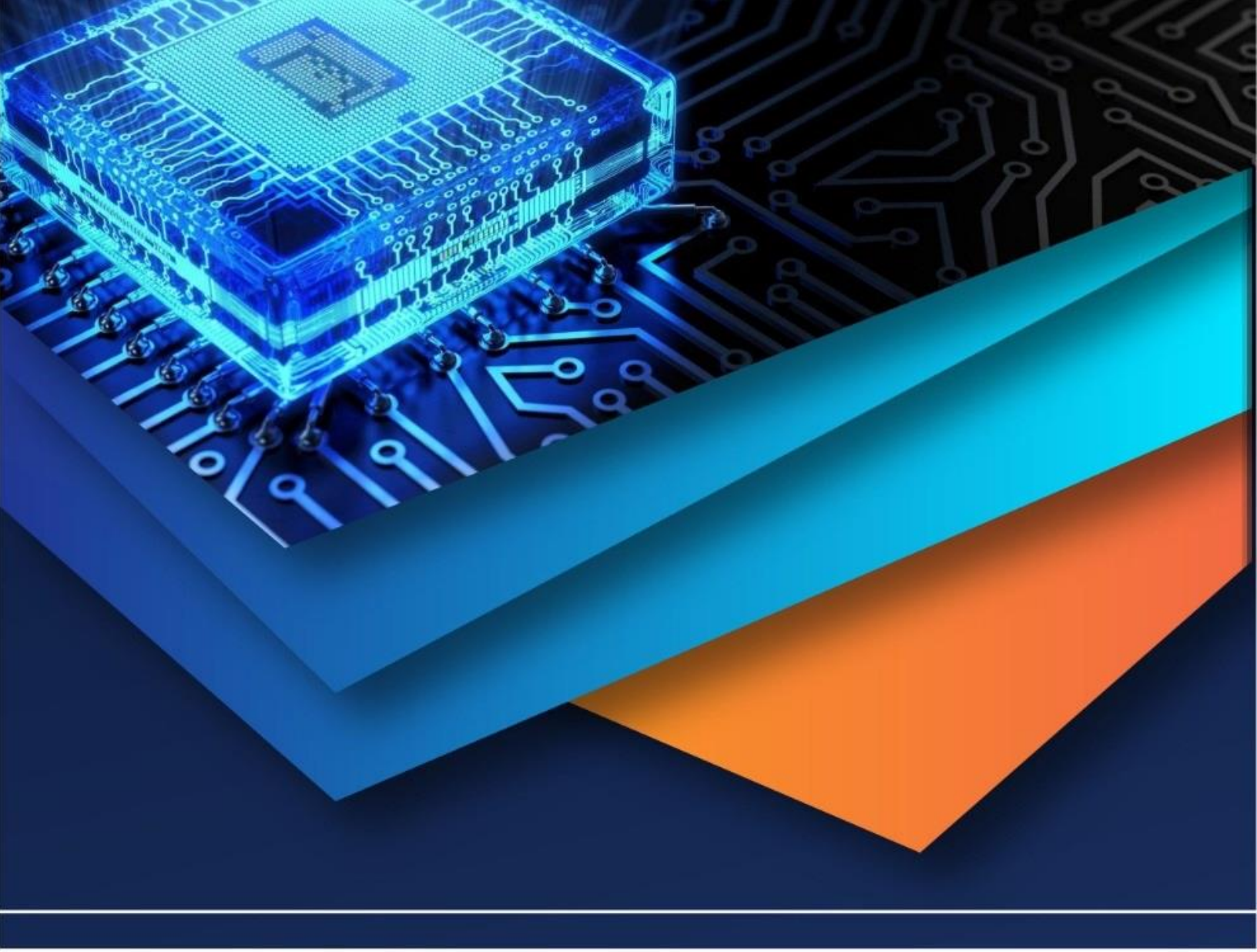
[14] Israat Tanzeena Haque Ioanis Nikolaidis Pawel Gburzynski, “On the Pitfalls of Directional Location–based Randomized Routing”, SPECTS 2007, July 16-18, San Diego, CA, USA.

[15] H. Kalosha, A. Nayak, S. Ruhrup, and I. Stojmenovic. Select-andprotest-based beaconless georouting with guaranteed delivery in wireless sensor networks. In Proceedings of the 27th IEEE International Conference on Computer Communications (INFOCOM), April 2008.

[16] Stefan Ruhrup, Hanna Kalosha, Amiya Nayak, and Ivan Stojmenovic;. 2010. Message-efficient beaconless georouting with guaranteed delivery in wireless sensor, ad hoc, and actuator networks. IEEE/ACM Trans. Netw. 18, 1 (February 2010), 95-108

[17] T. Winter, et. Al. “RPL: IPv6 Routing Protocol for Low power and Lossy Networks ” , March 13, 2011, available at: https://svn.tools.ietf.org/html/draft-ietf-roll-rpl-19.

[18] Shuhui Ma, Hong Ji, “An Energy-aware Geographical Routing Protocol in Wireless Sensor Networks”, International Conference on Communication Technology, ICCT '06 Guilin, China, Nov. 2006.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY