International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE www.irjcs.com

Survey on MANET's Mobility Models and Security Attacks for Routing Protocols

Mamatha C.R
Dept. of Computer Science and Engg., Vemana Institute of Technology, VTU

Ankit Chaurasia
Dept. of Computer Science and Engg., Vemana Institute of Technology, VTU

A.Rishi Akil
Dept. of Computer Science and Engg., Vemana Institute of Technology, VTU

***Abstract* — MANET is an infrastructure-less, dynamic network which have a group of wireless mobile nodes that send messages to each nodes in the group without any centralized authority. This paper is a survey paper and we talk about the routing protocols. Discussion has been done on the characteristics, challenges, applications, security goals and different types of security attacks on MANET. Ad hoc physical composition does not require an access point, it is simple to setup, particularly in a small or temporary network. Each node in the network sends the packet without any central administration. In ad hoc network, node acts as a router to receive and send the data. The advantage of the system is its robustness, flexibility and mobility. Ad hoc network are capable of analyze the radio broadcast environment to optimize the performance and it requires that nodes have capability to position as well as memory to go back over geographical local condition. The paper will also tell about the congestions in the Ad-hoc networks, and how we can rectify them using various Congestion mechanisms.**

I. INTRODUCTION

MANETs are wireless ad hoc networks that have a routable networking ambiance on top of a Link Layer ad hoc network. It consists of an end-to-end, self-forming, self-healing network as it includes the mobility of the nodes. Every single device in MANET is independent to move in any direction, and will hence, change its links to other devices often, and must route traffic different to its own use, and so, be a router. The major challenge in building a MANET is equipping each device to continuous maintain the data, required to route traffic. Such network may operate by itself or may be connected to the larger Internet. They may have one or more and other modules to receive or send, between mobility nodes. This causes in a highly dynamic, self-structure. The overall performance of any wireless protocol depends on the time of peer-to-peer connection between any two nodes transferring data as well on the time period of peer-to-peer connections between nodes of a data path containing n-hops. We will call these parameters averaged over entire network as "Average Connected Paths". The mobility of the nodes affects the number of average connected paths, which in turn affect the performance of the routing algorithm. With very thinly populated network the number of possible connection between any two nodes is very less and hence the performance is low. It is expected that if the degree of compactness of nodes are increased the turnout of the network shall increase, but beyond a certain level of compactness is increased the performance decreases in some protocol.

II. MANET'S CLASSIFICATION

The wireless network structure has two classes; first one is infrastructure where the node is attached with the one physical representation. Thus, the nodes are communicated through access points. Examples for these kinds of wireless networks are GSM, UMTS and WLAN etc. Second – infrastructure-less - where the node is conveyed without any fixed structural representation. MANETs are formed by connecting the terminals in the multi-hop distributed architecture. Due to the no presence of central structure, the nodes in the MANET behave as router to send and receive the data. Due to its non-static nature, MANET stops the single point of failure and makes the network robust.

III. CHARACTERISTICS OF MANET

Mobile Ad hoc Network is a group of autonomous and mobile elements such as laptops, smart phones, wearable computers, tablet, PC, PDA etc. The mobile nodes can vigorously self-organize in random fleeting network topology. Some chief descriptions of MANET are discussed below:

- *Infrastructure-less: MANET does not require any specialized hardware to make connection between nodes. All nodes communicate with each other through the wireless link.*
- *Multihop Routing: When nodes try to send data to among nodes which are out of their range of its contact, the packet shall be forwarded via one or more focused nodes.*

- *Autonomous Terminal: In MANET, each mobile node perform their own task alone, which could work either as a host or as a router.*
- *Dynamic Topology: Nodes are free to move arbitrarily in any direction with different speeds; thus, the network topology gets changed randomly at any time. The nodes in the MANET dynamically establish routing among them as they travel around and them establishing their own network.*
- *Light-Weight Terminals: In most of the cases, nodes used are mobile with less CPU capacity, low power storage and small memory size.*
- *Bandwidth-constrained and variable capacity links: Wireless links have lower capacity than their hard wired counterpart. Due to multiple admissions, noise, and interference situation, the capacity of a wireless link downgrade over a period of time and the effectual throughput may be less than the highest transmission capacity of radio transmitter.*

IV. UNDERSTANDING THE PERFORMANCE OF MOBILE NETWORKS

We try to estimate the maximum achievable performance of a mobile wireless network. Study of mobile networks is demanding as such study must be taken into account of the link volatility created by network for active as well as node mobility. Although a network is separated at a given time period, the routing can still be feasible if we see a time interval. We build on past work on time drawn out graphs and apply it to the study of mobile ad hoc networks. We also lessen the number of nodes in the time drawn out graph, and hence space obscurity of the study, by pruning the nodes that stay still over many intervals. We were able to scale the recitation analysis to hundreds of nodes.

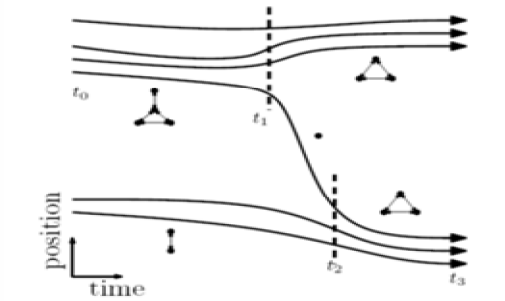

Figure 1. Understanding the performance of mobile networks

V. PREDICTIVE ROUTING FOR MOBILE SINKS

If the mobility of the mobile sink has some arrangement to it or is expected to some extent, we can exploit the knowledge about the path to perform predictive routing. We can re-route data to the relay nodes along the usual path of the mobile node, but not to the sink directly. The data stays on these nodes till the mobile node crosses and picks up the data. We use linear programming to find stashing nodes choices that reduce the communication overhead while guarantee heaviness against link and node failures, as well as path irresolution. We found that this technique achieves data delivery competence similar to what is possible with perfect knowledge about future trajectory of the mobile node.

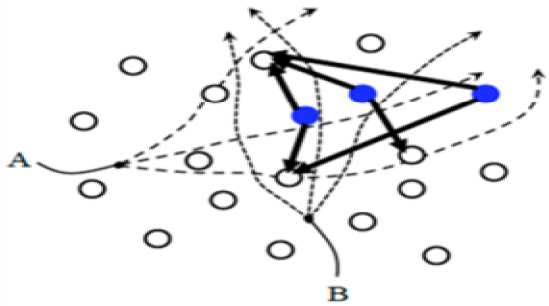

Figure 2. Predictive Routing To Mobile Sinks

VI. HIERARCHICAL ROUTING ROBUST TO SINK MOBILITY

To make data to be delivered to mobile sinks efficiently, our plan is to select them in a dispersed manner. A set of well-placed nodes which act as mediators between the data sources and clusters of nearby users. These intermediaries' nodes are chosen via the spread structure of HSTs, which are thin structures that make a natural spatial clustering of the network. The trees are doubter to the number and place of sources as well as to the routing patterns of users. Our thin and flexible infrastructure is precompiled and efficiently reused by sources and users, its cost repay over time.

The algorithm ensures, a certain stretch bound for the data delivery path with high possibility, and is healthy to lossy links and node failure by providing optional HST-included routes. Nearby users are gathered and their requests are aggregated which is without further falling communication overhead.

VII. MANET'S CHALLENGES

Mobility model in MANET face many challenges, namely:

(1) *Limited Bandwidth*
Wireless link carry on which have lesser capacity than infrastructure networks. In totalling, the realized result of wireless communication after accounting for the effect of many access, fading, noise, and interference conditions, etc. is often much less than highest transmission rate of a radiator.

(2) *Dynamic Topology*
Dynamic topology membership may disturb the faith relationship among nodes. The trust may also be not there if some nodes are found to be compromised.

(3) *Routing Overhead*
In wireless adhoc networks, nodes often change their location within network. So, some old routes are mapped in the routing table which leads to routing overhead which is unnecessary.

(4) *Hidden Terminal Problem*
This problem refers to the collision of packets at a receiving node due to the concurrent broadcast of those nodes that are not within the direct broadcast range of the sender, but are in the broadcast range of the losses of the receiver packet due to broadcast errors. MANETs experiences a much higher packet loss due to factors such as amplified collisions due to the presence of hidden terminals, presence of intrusion, uni-directional links, and common path breaks due to mobility of nodes.

(5) *Mobility-Induced Route Changes*
The network topology in an ad hoc wireless network is highly lively due to the movement of nodes; hence an on-going session suffers common path breaks. This situation often leads to changes most commonly in frequent nodes.

(6) *Battery Constraints*
Devices used in these networks have limits on the power supply sources in order to maintain mobility, size and weight of the device.

(7) *Security Threats*
The wireless mobile ad hoc nature of MANETs brings new safety challenges to the network plan. As the wireless medium is weak to eavesdropping and ad hoc network functionality is recognized through node assistance, mobile ad hoc networks are essentially bare to numerous security attacks.

VIII. MOBILITY MODELS

Different mobility models can be distinguished according to their spatial and temporal dependencies.

(1) *Spatial Dependency*
It is a measure of how a couple of nodes are dependent in their motion. If a couple of nodes are moving in same motion then they have high spatial dependency.

(2) *Temporal Dependency*
It is a measure of how current velocities (magnitude and direction) are related to previous velocities. Nodes having same speed have high temporal dependency.

(3) Random Waypoint
The Random Waypoint model is the most often used mobility model in research community. At every instance, a node randomly opts a destination and moves towards it with a velocity opted randomly from a uniformly spread [0, V_max], where V_max is the maximum allowed velocity for every mobile node. After it reaches the destination, the node stops for a period defined by the 'pause time' parameter. After this duration, it again opts a random destination and loops the whole process until the simulation comes to an end. The simulation though gave the approximate idea about the result and the behaviour of the node and packet transmission, there are chances of the nodes failure and packet drop which the simulation results vaguely showed or did not mentioned.

(4) Random Point Group Mobility (RPGM)
Random point group mobility can be used for communication in military battlefield. Here each group has a logical leader that determines the motion behavior of the group. At first, each member of the group is uniformly distributed in the neighborhood of the group leader. Pronominally, at each period of time, every node has speed and direction that is derived by randomly deviating from that of the group leader. The scenario contains sixteen nodes with Node 1 and Nodes as group leaders. SDR is the Speed Deviation Ratio and ADR is the Angle Deviation Ratio. The proposed theory [JDIM3] was mainly for the military purpose and showed that each node deviates from its velocity (both speed and direction) randomly from that of the leader. The movement in group mobility can be shown as follows:

$$|Vmember(t)|=|Vleader(t)|+random()*SDR*max\_speed \quad (1)$$
$$|\Theta member(t)|= |\Theta leader\ (t)| + random()*ADR*\ max\_angle \quad (2)$$

Where, 0 <<< 1. SDR and ADR are used to control the deviation of the velocity of collective members from that of the logical group leader. Since the group leader mainly decides the manoeuvrability of group members, group manoeuvre pattern is expected to have high spatial dependence for minute values of SDR and ADR. But again the model was tested for the limited number of the nodes and it did not predict the tested results for the behaviour of the model or the real time scenario consisting multiple hops and networks and is only valid for the smaller group of nodes dependent on the primary node.

(5) Freeway Mobility Model

This model simulates the motion behaviour of mobility nodes on a freeway or path. It can be used to exchange traffic status or can be used to track a vehicle on a freeway or path. Each mobile node is restrained to its lane on the freeway. The velocities of mobile nodes are temporally dependent on its previous velocities. The model failed to capture the present scenario of the traffic which can be intercepted by the external network agent or can be hacked, so there is no security provided for the network. And also restricting the nodes to the lane restricts the dynamic working behaviour for transferring the data. Hence, shows high spatial dependency with dependence of velocity relating to previously node.

(6) Manhattan Mobility Model

We introduce the Manhattan model to simulate the movement pattern of mobile nodes on streets. It can be used in modelling motion in an urban area .The scene is composed of a number of horizontal and vertical streets. The map defines the roads along the nodes can move. Maps are used in this model too. However, the map is composed of a number of horizontal and vertical streets. The mobile node is allowed to move along the line of horizontal and vertical paths on the map. At the crossroad of a horizontal and a vertical street, the mobile node can turn left, right or go straight with certain probability. Except the above difference, the node relationships involved in the Manhattan model are the same as in the Freeway model. This model certainly overcome the constraints in the Freeway mobility model but has geographic restrictions.

IX. SECURITY GOALS IN MANET

All networking functions such as routing and packet sending, are done by nodes itself in a self-organizing form. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to assess if mobile ad-hoc network is safe or not are as follows:

- *Availability: It means the properties are available to rightful parties at right times. Ease of use applies both to data and to services. It ensures the endurance of network service in spite of DoS attack.*
- *Confidentiality: It ensures that computer-related properties are accessed only by rightful parties. Guards of information which is exchanged through a MANET. It should be sheltered against any leak attack like eavesdropping-unauthorized reading of message.*
- *Integrity: It means that properties can be modified only by official parties or only in authorized way. Integrity assures that a message being transferred is never tainted.*
- *Authentication: It is essentially pledge that member in message are real and not mimic. The recourses of network should be accessed by the genuine nodes.*
- *Authorization: This attribute assigns different access rights to various types of users, for example a network management can be executed by network administrator only.*
- *Resilience to attacks: It is required to maintain the network functionalities when a portion of nodes is compromised or cracked.*
- *Freshness: It ensures that harmful node does not resend previously captured packets.*

X. DESCRIPTION OF ROUTING PROTOCOL

In practice we have the following routing protocols:

(1) Destination-Sequenced Distance-Vector (DSDV)

This Routing protocol is a practical table driven algorithm based on classic Bellman-Ford routing. In practical protocols, all the nodes study the network topology before a forward request comes in. In DSDV protocol each node maintains routing in series for all known destinations. The routing information is well prepared timely. Each node maintains a table, which has information for all accessible destinations, the next node to reach the destination, number of hops to reach the destination and sequence number. The nodes occasionally send this table to all neighbours to maintain the network topology, which augments to the network overhead. Each entry in the routing table is noticed with a sequence number assigned by the destination node. The sequence numbers allow the mobile nodes to differentiate old routes from new ones, thereby avoiding the configuration of routing loops.

(2) Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is a hasty protocol i.e. it determines the proper route only when a packet needs to be sent. The node fills the network topology with a routing request and establishes the required route from the responses it receives.

DSR allows the network to be totally self-configuring without the need for any accessible network infrastructure or administration. The DSR protocol comprises of two main mechanisms that work hand in hand to allow the finding and upholding of source routes in the ad hoc network. All aspects of protocol operate entirely on demand, which allows the routing packet overhead of DSR to scale up automatically by itself. Route Sighting is when a source node S wishes to send a packet to the destination node D, it obtains a route to D. This is called Route Sighting. It is used only when S attempts to send a packet to D and has no in rank on a route to D. Route Maintenance is when there is a change in the network topology, the offered routes can no longer be used. In such a scenario, the source S can use an optional route to the destination D, if it knows one, or invoke Route Sighting. This is called Route Maintenance.

XI. CLASSIFICATION OF SECURITY ATTACKS

The attacks can be classified on the basis of behavior of the attack i.e. Passive or Active attack.

(1) Passive Attacks

It does not alter the data sent within the network. But includes the unauthorized detection to the network traffic or collect data from it. Passive attacker does not disrupt the functionality of a routing protocol but attempts to finds the important data from sent traffic.

(2) Active attacks

Active attacks are very harmful attacks on the network that stop messages from flowing between the nodes, active attacks can be internally or externally. Active external attacks can be carried out by the sources that do not belong to the network. Internal attacks are from harmful nodes which are part of the network, internal attacks are more stern and hard to detect than external attacks. These attacks generate prohibited access to network that helps the attacker to implement changes such as modification of packets, DoS, congestion etc. Active attacks are classified into four groups:

- Dropping Attacks: Affected nodes or selfish nodes can drop all packets that are not intended for them. Declined attacks can prevent end-to-end communications between nodes.
- Modification Attacks: These attacks changes packets and interrupt the entire message between network nodes. Sinkhole attacks are the example of modification attacks.
- Fabrication Attacks: In this type of attack, the attacker sends false messages to the neighbouring nodes without receiving any related message.

The uniqueness of MANETs makes them vulnerable to many new attacks. These attacks can initiate in different levels of the network protocol stack.

(1). *Attacks at Physical Layer*

Some of the attacks recognized at physical layer comprise eavesdropping, interference, and jamming etc.

- Eavesdropping: It can also be defined as interference and analysis of messages and conversations by not deliberate receivers. The main aim of such attacks is to get the private information that should be kept covert during communication.
- Jamming: Jamming is a special class of DoS attacks which are initiated by infected node after shaping the range of communication. Overcrowding attacks also prevents the reception of legitimate packets.
- Active Interference: An active intrusion is a denial of service attack which blocks the wireless communication channel.

(2). *Attacks at Data link layer*

The data link layer can be categorized as attacks as to what effect it has on the state of the network as a whole.

- Selfish Misbehaviour of Nodes: The selfish nodes may ignore to take part in the forwarding process or drops the packets purposely in order to save the resources and to preserve the battery power.
- Malicious Behaviour of nodes: The main job of harmful node is to disturb normal operation of routing protocol. The impact of such attack is amplified when communication takes place amongst neighbouring nodes. Attacks of such type are fall into following category:
- Denial of Service (DoS): bring to a halt of authorized access to resources or suspending of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by a mugger to stop rightful users of a service from using the preferred resources and attempts to flood a network, thereby stopping genuine network traffic.
- Misdirecting traffic: A harmful node advertises false routing information in order to get protected data before the original route.
- Attacking neighbor sensing protocols: harmful nodes advertise false error messages so that important links disruption are marked as broken.

(3). *Attacks at Network Layer*

The basic idea about network layer attacks is to insert itself in the active path from source to destination or to absorb network traffic.

- Blackhole Attack: In this type of attacks, harmful node claims having the most favorable route to the node whenever it gets RREQ packets, and sends the REPP with highest destination sequence number and least hop count value to creator node, whose RREQ packets it wants to access.

- Rushing Attack: In rushing attacks when compromised node receives a route request packet from the source node, it floods the packet as soon as possible, throughout the network before other nodes, which also receive the same route request packet.
- Wormhole Attack: In wormhole attack, harmful node receive data packet at one point in the network and attach them to another harmful node. The tunnel exist between two harmful nodes is referred to as a wormhole.
- Grey hole attack: In this type of attacks, harmful node claims having an most favored route to the node whose packets it wants to cut off. It is almost same as Blackhole attack but it drops data packet of a particular node.
- Sinkhole Attack: In sinkhole Attack, a compromised node or harmful node sends wrong routing in turn to create itself as a particular node and get whole network traffic. After getting whole network traffic it manipulates the secret information, such as changes made to data packet or drops them to make the network intricate. An infected node tries to attract the protected data from all neighboring nodes.

(4). *Attacks at Transport Layer*

Session Hijacking: Here attacker takes the benefit to utilize the insecure session after its initial setup. In this attack, the attacker take off IP address of node of the victim, finds the exact sequence number i.e. expected by the target and then creates different DoS attacks.

(5). *Attacks at Application Layer*

- Malicious code attacks: It includes, Viruses, Worms, can attack both operating system and user application, which augments to the network overhead. Each entry in the routing table is noticed with a sequence number assigned by the destination node. The sequence numbers allow the mobile nodes to differentiate old routes from new ones, thereby avoiding the configuration of routing loops. The
- Dynamic Source Routing (DSR)**:** Dynamic Source Routing protocol is a hasty protocol i.e. it determines the proper route only when a packet needs to be sent. The node fills the network topology with a routing request and establishes the required route from the responses it receives. DSR allows the network to be totally self-configuring without the need for any accessible network infrastructure or administration. The DSR protocol comprises of two main mechanisms that work hand in hand to allow the finding and upholding of source routes in the ad hoc network. All aspects of protocol operate entirely on demand, which allows the routing packet overhead of DSR to scale up automatically by itself.
- Route Sighting: When a source node S wishes to send a packet to the destination node D, it obtains a route to D. This is called Route Sighting. It is used only when S attempts to send a packet to D and has no in rank on a route to D.
- Route Maintenance: When there is a change in the network topology, the offered routes can no longer be used. In such a scenario, the source S can use an optional route to the destination D, if it knows one, or invoke Route Sighting. This is called Route Maintenance.

XII. CONCLUSION

In this paper we tried to analyse how exactly MANET works and how it is prone to threats. Its intrinsic flexibility, absence of infrastructure, ease of positioning, auto configuration, low cost and potential applications makes it important part of further common calculating environments. Empirical results shows that the performance of routing rules varies widely across different mobility models and therefore, the study results from one model cannot be applied to other model. Hence we have to consider the mobility of an application while selecting a routing protocol. The main aim of routing protocol is to provide efficient energy cognizant and secure routing theory to MANET. After that we discuss the most complicated and challenging issue in MANET i.e. Security with their goals and Attacks (passive and Active). The researchers put a lot of effort to find to the problems being faced by the users and the sender sending the information over the network, the main concern would be to try to eliminate the threat to the data and protect the information. This review aims to discover ad hoc network structure, application, and mien and also mentions about different challenging issues and provides the correct solution based on new technology. Hence, MANET is a fast developing and changing field with a huge scope of research work in this field and future study should be conducted to compare protocols in low mobility environment, where routes do not break to too often. Dedicated protocols may give better performance for near secure environment. Designing views which depict real world applications more precisely can be designed through in-depth study of the application.

REFERENCES

[1] D. Helen* and D. Arivazhagan, "*Applications, Advantages and Challenges of Ad Hoc Networks*", Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014 (ISSN: 2278-5213).

[2] Meenakshi Yadav1 , Nisha Uparosiya2, "*Survey on MANET: Routing Protocols, Advantages, Problems and Security*",International Journal of Innovative Computer Science & Engineering,2014 (ISSN: 2393-8528).

[3] Prabhleen Kaur, Sukhman, *" An Overview on MANET- Advantages, Characteristics and Security Attacks",* International Journal of Computer Applications (0975–8887), 4th International Conference on Advancements in Engineering & Technology (ICAET 2016).

[4] Bhavyesh Divecha1 , Ajith Abraham2 , Crina Grosan2 and Sugata Sanyal3, "*Impact of Node Mobility on MANET Routing Protocols Models"*.
[5] Manoj Kumar Singh, Sujata Negi Thakur, *"Comparison of DSDV, DSR and ZRP Routing Protocols in MANETs",* International Journal of Computer Applications (0975 – 8887) Volume 108 – No. 13, December 2014.
[6] Md. Mahbubul Alam, Tanmoon Taz Shetu, A report submitted to Sadia Hamid Kazi of Computer Science and Engineering Department of Brac University in fulfilment of the requirements for thesis work, April-2011.
[7] Aarti,Dr. S. S. Tyagi, *"Study of MANET: Characteristics, Challenges, Application and Security Attacks*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 (ISSN: 2277 128X).
[8] Shailesh P. Patil, Pankaj R. Chandre, *"Trust and Neighbor Coverage Based Protocol to Improve Reliability of Routing in MANET"*, 2016 International Conference on Computing Communication Control and automation (ICCUBEA).
[9] Sharad Awatade, Shweta Joshi, *"Improved EAACK: Develop Secure Intrusion Detection System for MANETs Using Hybrid Cryptography"*, International Conference on Computing Communication Control and automation (ICCUBEA), 2016.
[10] Yugandhara S. Patil , Dr. Ashok M. Kanthe , *"Gray Hole Attack Detection using False Reply Count and TrueLink based Path Authentication in MANET"*, International Conference on Computing Communication Control and automation (ICCUBEA), 2016.
[11] Arik Motskin, Ian Downes, Branislav Kusy, Omprakash Gnawali, and Leonidas Guibas, *"Network Warehouses: Efficient Information Distribution to Mobile Users"*, To appear in proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM 2011), April 2011. Acceptance Rate-291/1823.
[12] Ian Downes, Branislav Kusy, Omprakash Gnawali, and Leonidas Guibas, *"Interactive Analysis and Simulation of VANETs Using MOWINE"*, The IEEE Vehicular Networking Conference (VNC 2010), December 2010.
[13] HyungJune Lee, Martin Wicke, Branislav Kusy, Omprakash Gnawali, and Leonidas Guibas, *"Data Stashing: Energy-efficient Information Delivery to Mobile Sinks through Trajectory Prediction"*, In Proceedings of the ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 2010), Stockholm, Sweden, April 12-16, 2010. Acceptance Rate - 20/117.

