International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

PRIVACY PRESERVING DATA SHARING WITH ANONYMOUS ID ASSIGNMENT

P. Jayalakshmi* & R. Selvakumar**
* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

Introduction:

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

Module Description:

- ✓ WSN Configuration And Setup
- ✓ Multi Hop Tree Network
- ✓ Virtual Coordinates Location Module
- ✓ Computation Of Paths For Topology
- ✓ Resultant Paths – Security
- ✓ Modules – Revocation

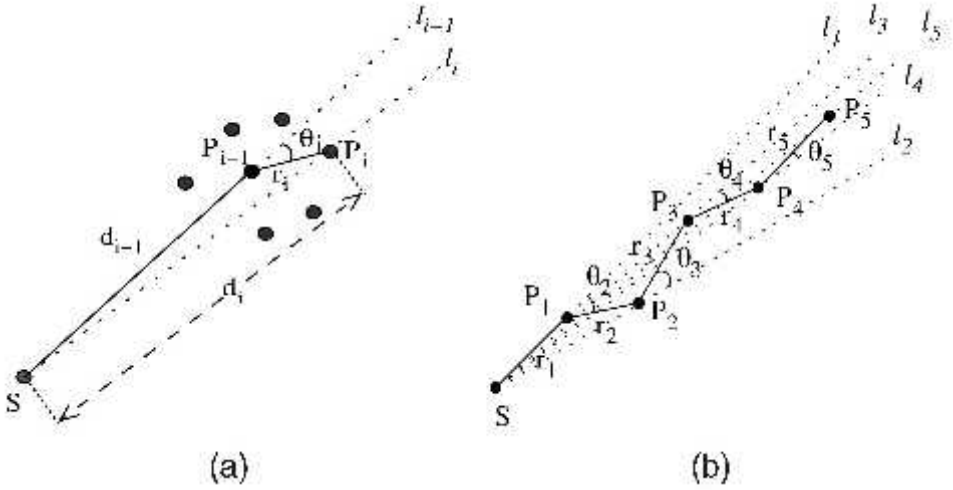
WSN Configuration and Setup:

The WSN are placed in a remote locations with a sink connected to the network. According to the number of cluster heads, the nodes are randomly placed in a network. As events occur randomly the WSNS transmit the data's to the sink node or master node. Each node is assumed to be calculating the energy independently. The data transmission takes places. Whenever the particular node is used for data transmission, an energy level should be reduced. The WSNs which act as relays also lose energy when relaying the data's of the WSN's. Thus each node is acting independently when event occurs and transmits energy according to differing energy levels.

Multi Hop Tree Network Module:

We Make the Following Assumptions in Our Model:

- ✓ Nodes are stationary in the WANET.
- ✓ Each node in the WANET uses Omni-directional antennas.
- ✓ Each node knows the distance between itself and its neighboring nodes using distance estimation



The nodes between two randomly located sensors are analytically computed via iteration based on expressions for connectivity in one or two hops. In, the distribution of hop distance and its expected value are analyzed with simulations. It is shown that beam forming antennas significantly reduce the hop distance compared to Omni-directional antennas for medium and large networks with random node locations.

Virtual Coordinates Location Module:

The set of VCs has the connectivity information embedded in it, though it has no directional information. All the nodes that are hops away from the anchor have as the coordinate. Each ordinate propagates as a concentric circle centered at the corresponding anchor, while the angular information is completely lost.

The random node locations in the proposed method is based on restricting the propagation direction outward from the propagation source in each hop and greedily searching the furthest neighbor each time for each topology, a single sample multi hop path is selected for each hop distance n. Second, we place the source node at randomly selected locations and vary the node density. Similarly, one can form 2,000 independent topologies for each node density value the effect is a decrease in the expected multi hop Euclidean distance of a randomly chosen n-hop path. In the simulations, it is observed that the reduction in the multi hop Euclidean distance is largely caused by the decrease in the distance taken in the final hop under the edge effects.

Computation of Paths for Topology:

Distance estimation the results demonstrate that for a smaller node density, the edge effect is less pronounced. This is an expected result since the edge effect reduces the final hop distance of a multi hop path, which has a stronger limitation on higher densities with larger single-hop spans. As the node density gets smaller, the node with the maximum distance in the final hop is located closer to the most recently selected node and its location is limited less frequently by the topology border.

The diminishing character in the average percent error values is caused by the decrease in the ratio between the amounts of distance in the final hop to the multi hop path distance as the hop distance increases. Thus the computation of new paths Introduction of new nodes or mobility of nodes cause major changes and this cause the network topology can render the TPM inaccurate thus requiring its re-computation. If the change in the connectivity pattern is completely localized. Thus estimate the TCs of a new node based on some localized computations involving its immediate static neighbors.

Resultant Paths – Security:

The unit disk model defines the communication range as the minimum radius of a circular reception area within which all transmissions are successfully received if no interference or packet collisions exist. In the event that the wireless medium is subject to the effects of fading, the reception power at receiver nodes is affected by the distance to the transmitter and decays exponentially with distance. Furthermore, with the presence of Gaussian noise, the received power becomes a random variable. This makes the reception of a packet a probabilistic event dependent on the distance to the transmitter node, the statistical characteristics of the channel noise, transmission power, and the threshold of reception power.TPM presents a robust, accurate, and scalable alternative to physical map generation or localization. The adversary or attacker launches a attack. The attack compromises a few nodes only and this in turn uses the cryptographic information obtained from the compromised nodes. The attack is thus detected and then nullified. This is done by the replica node in the topology.

Existing System:

- ✓ Major problems of WSN in underwater acoustic communications are low data rates and long transmission delays.
- ✓ Very few works have been done to determine how the anchors should transmit their packets to the sensor nodes.
- ✓ In long base-line (LBL) systems where transponders are fixed on the sea floor, an underwater node interrogates the transponders for round-trip delay estimation. In the underwater positioning scheme, a master anchor sends a beacon signal periodically, and other anchors transmit their packets in a given order after the reception of the beacon from the previous anchor.
- ✓ The localization algorithm addresses the problem of joint node discovery and collaborative localization without the aid of GPS. The algorithm starts with a few anchors as primary seed nodes, and as it progresses, suitable sensor nodes are converted to seed nodes to help in discovering more sensor nodes.
- ✓ In previous work, we considered optimal collision-free packet scheduling in a UASN for the localization task in single-channel (L-MAC) and multi-channels canaries (DMC-MAC). In these algorithms, the position information of the anchors is used to minimize the localization time. In spite of the remarkable performance of L-MAC and DMC-MAC over other algorithms (or MAC protocols), they are highly demanding.

Disadvantages:

- ✓ GPS signals (radio-frequency signals), however, cannot propagate more than a few meters, and underwater acoustic signals are used instead.
- ✓ In addition, radio signals experience negligible propagation delays as compared to the sound (acoustic) waves.
- ✓ There is no guarantee that it will perform satisfactorily for the localization task.
- ✓ The main drawback of L-MAC or DMC-MAC is that they require a fusion center which gathers the positions of all the anchors, and decides on the time of packet transmission from each anchor. In addition, these two collision-free algorithms need the anchors to be synchronized and equipped with radio modems to exchange information fast.

Proposed System:

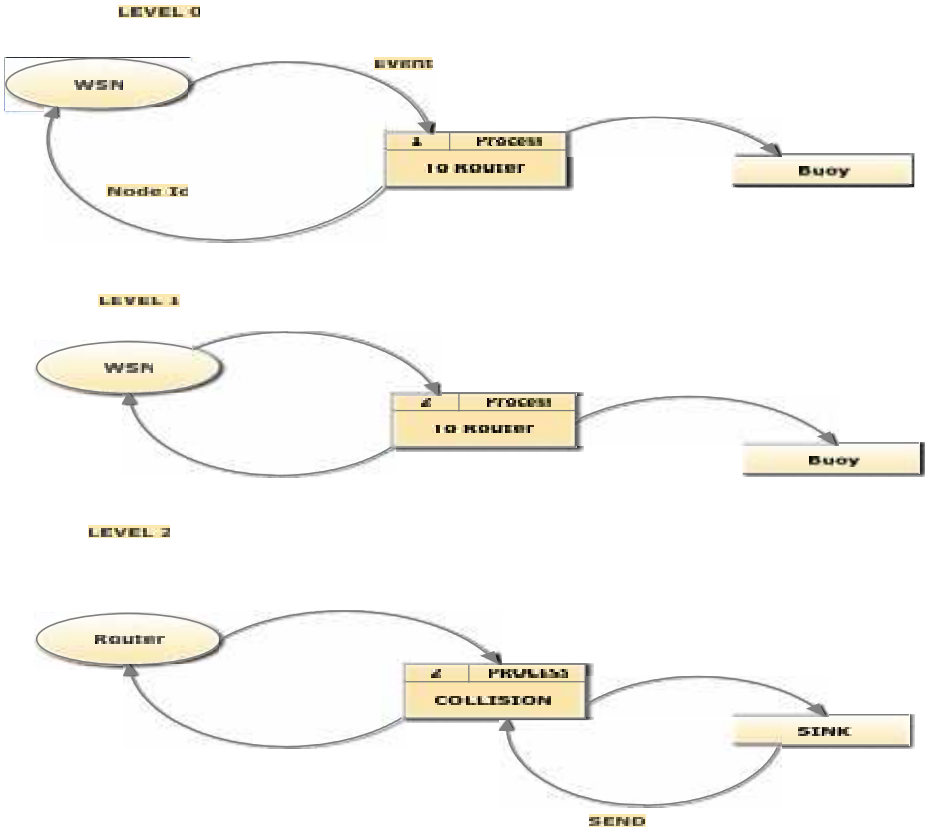
- ✓ The model considers packet scheduling algorithms that do not need a fusion center.

- ✓ Although the synchronization of the anchors which are equipped with GPS is not difficult, the proposed algorithms can work with synchronized anchors if there is a request from a sensor node.
- ✓ We assume a single-hop UASN where anchors are equipped with half-duplex acoustic modems, and can broadcast their packets based on two classes of scheduling: a collision-free scheme (CFS), where the transmitted packets never collide with each other at the receiver, and a collision-tolerant scheme (CTS), where the collision probability is controlled by the packet transmission rate in such a way that each sensor node can receive sufficiently many error-free packets for self localization.

Advantages:

Assuming packet loss and collisions, the localization time is formulated for each scheme, and its minimum is obtained analytically for predetermined probability of successful localization for each sensor node.

- ✓ A shorter localization time allows for a more dynamic network, and leads to a better network efficiency in terms of throughput.
- ✓ It is shown how the minimum number of anchors can be determined to reach the desired probability of self localization.
- ✓ An iterative Gauss-Newton self-localization algorithm is introduced for a sensor node which experiences packet loss or collision. Furthermore, the way in which his algorithm can be used for each packet scheduling scheme is outlined. The Cramér Rao lower bound (CRB) on localization is derived for each scheme. Other than the distance-dependent signal to noise ratio, the effects of packet loss due to fading or shadowing, collisions, and the probability of successful self-localization are included in this derivation.



DFD Diagram:

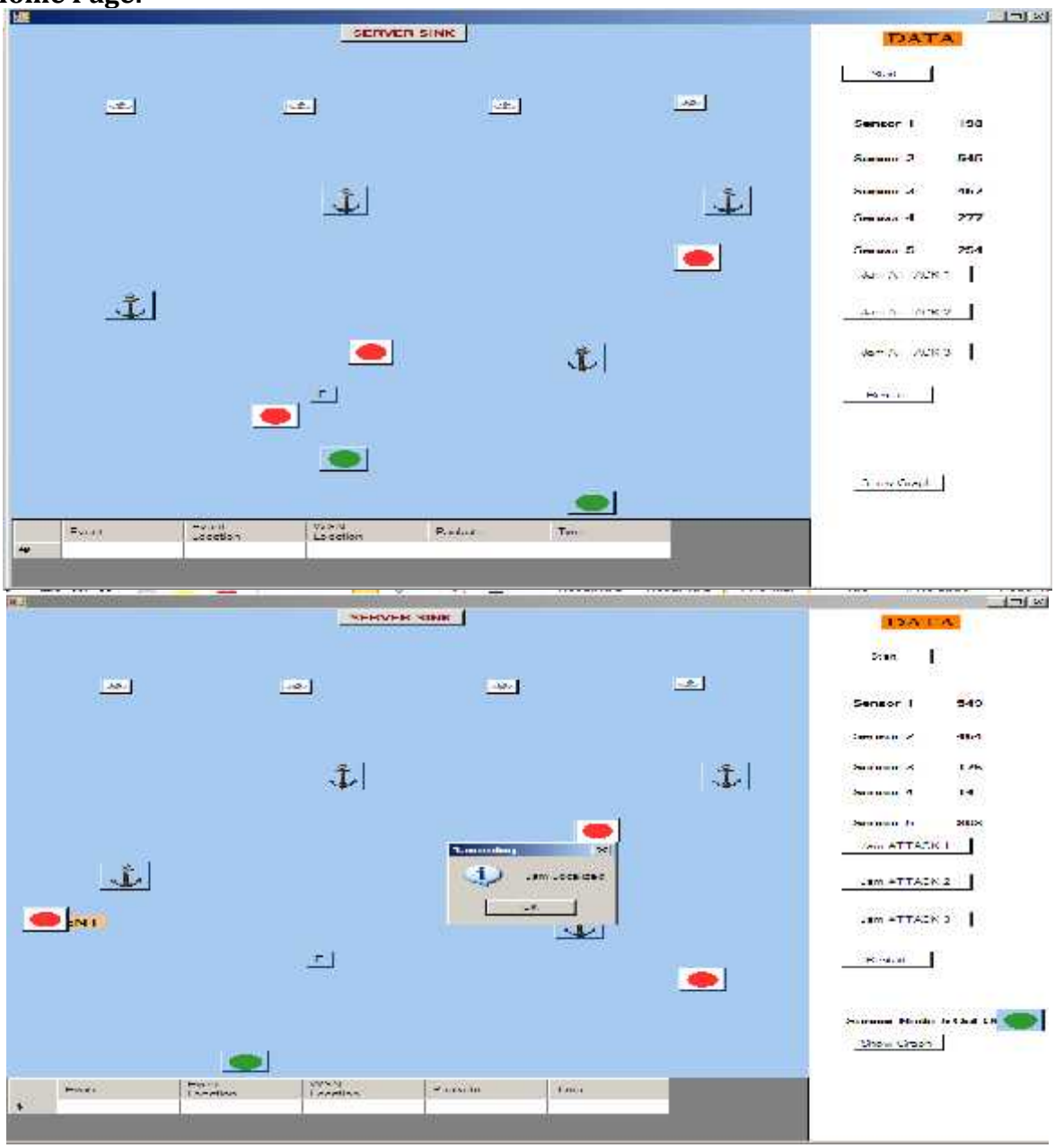
System Implementation:

In a wireless sensor network there are various possible security threats encountered. This paper is involved with combating two types of attacks: the compromised-node (CN) attack and the denial-of-service (DOS) attack. The CN attack refers to the situation when an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the WSN by actively disrupting, changing, or even destroying the functionality of a subset of nodes in the system. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. Other possible inclusions are energy harvesting modules, secondary ASICs, and possibly secondary communication devices

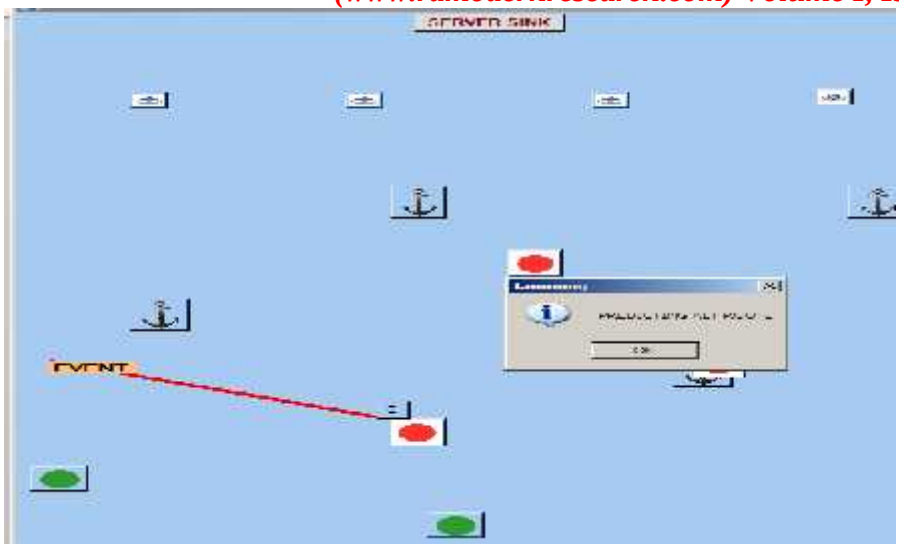
These two attacks are similar in the sense that they both generate *black holes*: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. A conventional cryptography-based security method cannot alone provide satisfactory solutions to these problems. This is because, by definition, once a node is compromised, the adversary can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. At the same time, an adversary can always perform certain form of DOS attack (e.g., jamming) even if it does not have any knowledge of the crypto-system used in the WSN

Screen Shots:

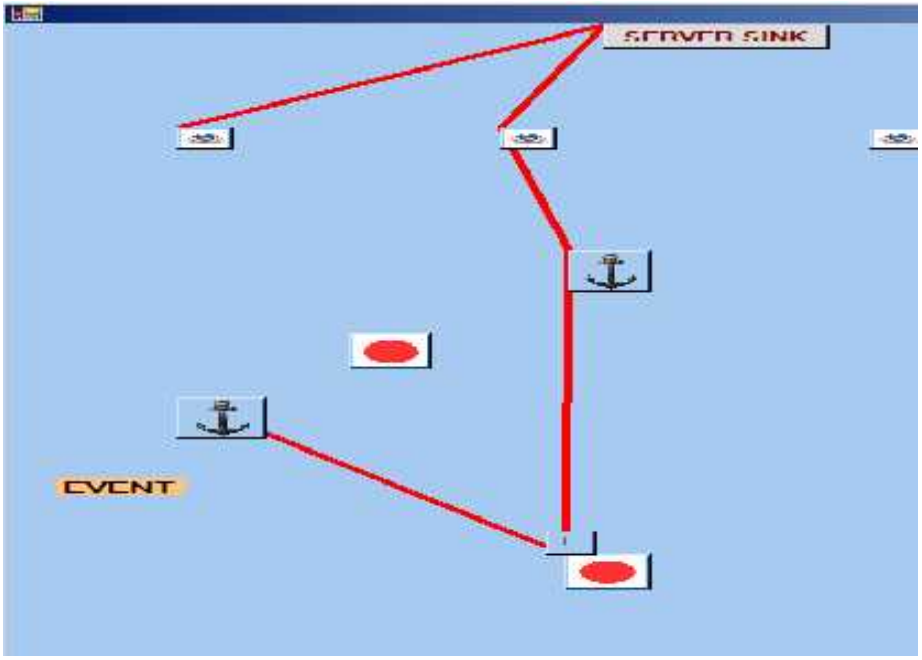
Home Page:



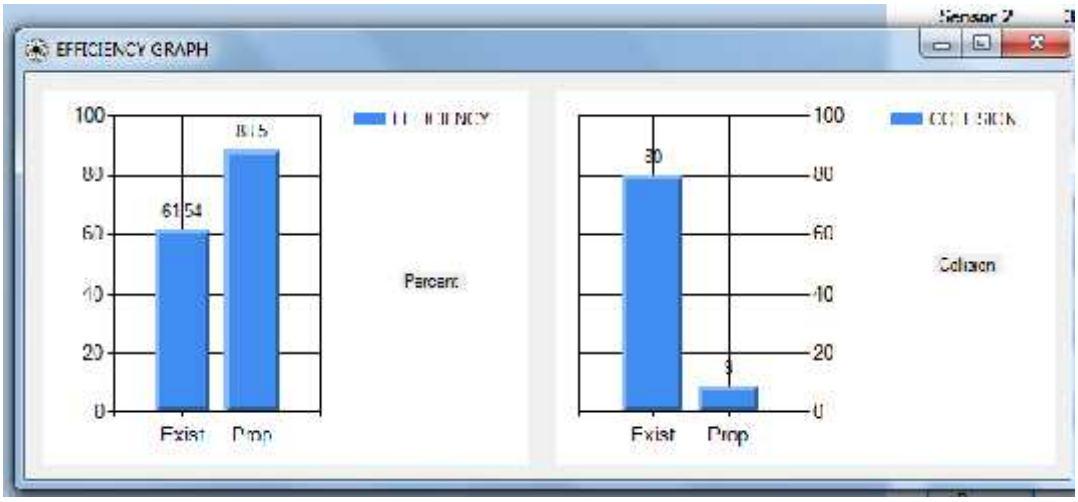
Jam Localized:




Jamming
PREDICTING INTERMEDIATE
OK



	Event	Event Location	WSN Location	Packets	Time
▶	Ship Event	X : 23 Y : 439	X : 254 Y : 512	12	579.956ms
*					



Conclusion:

Thus the results have shown the effectiveness of models which are very cost effective and secure with less energy consumption and also the ability to withstand attacks by nodes. By appropriately setting the correct virtual path and measures using Virtual coordinates the packets dispersion and congestion can be avoided. The novel model is also able to handle attacks by the adversaries including cloning attacks which are completely blocked. Energy consumption can further be reduced by the proposed algorithms to as low as 10¡3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multi-path routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy.

Future Work:

In future the randomized dispersive routing mechanism can be used in regular network protocols. The project can also be further enhanced to improve the energy efficiency with lower costs. The node density costs are also not escalated.

Further black holes elimination and avoidance can be done in all type of network topologies like virtual private networks, peer to peer; multilink downloads etc in a similar fashion as done in wireless sensor networks. Additionally the methods can be enhanced to prevent DOS attacks in futuristic models effectively.

References:

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, Aug. 2002.
2. C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA), pages 122–131, 2003.
3. M. Burmester and T. V. Le. Secure multipath communication in mobile ad hoc networks. In Proceedings of the International Conference on Information Technology: Coding and computing, pages 405–409, 2004.
4. P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. IEEE/ACM Transactions on Networking, 15(6):1490–1501, Dec. 2007.
5. X. Y. Li, K. Moaveninejad, and O. Frieder. Regional gossip routing wireless ad hoc networks. ACM Journal of Mobile Networks and Applications, 10(1-2):61–77, Feb. 2005.
6. W. Lou and Y. Kwon. H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transactions on Vehicular Technology, 5(4):1320–1330, July 2006.
7. W. Lou, W. Liu, and Y. Fang. Spread: enhancing data confidentiality in mobile ad hoc networks. In Proceedings of the IEEE INFOCOM Conference, volume 4, pages 2404–2413, Mar. 2004.