# A Review on Secure and Reliable Routing in Mobile Ad hoc Network under Flooding Attack

[1]Hardik Vyas
[1]Student
[1]Marwadi Education Foundation

***Abstract* - MANET (Mobile Ad-Hoc Networks) is a fastest growing network system and it offers many features to routing protocols and communication policies. Theses routing protocols are presented to avoid the attacker nodes and offers the effective interaction between source and destination. The attacks in the wireless or Mobile AdHoc network scenarios are: Blackhole attacks, Wormhole attack, DOS, Sniffing, Sybil and so on.**

***keywords* - Wired, wireless, secure, attack, protocols.**

## I. INTRODUCTION

Late advances in small scale preparing, battery and remote revolution, and keen sensors have improved data handling [3], [11], [13], remote correspondence as well as recognition capacity. In sensor arranges, each sensor hub has controlled remote computational energy to transfer as well as process the conscious information on the base station or data buildup concentration [2], [5], [8]. Hence, to build the transmission region as well as the sensor zone and [1], [12], the remote sensor manage more often than not contains several sensor hubs. For the maximum part, each sensor hub has a reduced quality of battery control which cannot be renewed. At the stage when the strength of a sensor hub is exhausted, remote sensor organize holes would emphasize, and also the fizzled hubs will not transport data to alternative hubs amid transmission management. Subsequently, another sensor hub would be troubled through extended transmission controlling. This work recommends a blame hub recuperation (FNR) computation to advancement the remote sensor's lifetime arrange (WSN) when a percentage of the sensor hubs close down, either in light of the fact which they never again have battery energy or they have achieved the functioning limit of theirs. By using the FNR computation is able to bring about fewer replacements of sensor hubs along with more recycled directing. This way, the computation promotions the WSN lifetime and diminishes the price of supplanting the sensor hubs.

Cyber Security: In recent decades, communications and computing have undergone amazing changes. In communicating, Computation is preferred on the go with a vast demand of mobility support [29, 30]. Because of huge user's quantity in wireless environment communication paradigm have shifted to the idea of Cognitive Radio Networks [27, 28] for improved use of wireless spectrum. Needless to say, the advancement in tremendous popularity and hand-held tool of mobile application leads to need of regular security and analysis provisioning of communication environment.

Flooding assault is one such assault which devours more asset like data transfer capacity, battery control, and so on.

Noteworthy works have been done in securing the impromptu system. It is tending to the aversion of flooding assault in the specially appointed system. Here we concentrate on flooding assault safeguard systems [7].

***DDOS Defense Mechanisms [7]***

### *A. DDoS defense mechanisms based on deployment*

This grouping depends on the area of usage of resistance system. This can additionally be classify as source based, goal based and arrange based

**Source based:** Here the instruments are conveyed close to the wellsprings of assault. These components essentially concentrate on confining the system clients from creating DDoS assaults. There are different components that are source based, some real one's are:

- Ingress/Egress sifting at source's edge switch: These strategies are proposed to identify the bundles with parodied IP address at the source's edge switch.
- D-WARD: D-WARD is a DDo Sdefense framework sent at source-end arranges that independently identifies and prevents assaults starting from these systems.
- MANA net's turn around firewall: Reverse firewall works uniquely in contrast to a conventional firewall. It restricts the rate at which it advances the parcels which are not answers.

**Goal based**: Under this classification, components are sent close to the casualty i.e. either at the edge switch or the entrance switch of the goal.

- IP Traceback systems: A method to recognize the root of the ridiculed client is known as the IP Traceback.
- Packet checking and separating components: In this plan, true blue bundles are stamped so that at the victi's side, a distinction can be made amongst honest to goodness and assault parcels. There are a few approaches to execute these instruments for instance, history-based IP separating, Hop-check sifting, Path identifier, bundle dropping in light of the level of clog.

**System based:** These instruments are for the most part conveyed inside systems and on the switches of the self-governing frameworks. A portion of the system-based guard instruments are course-based bundle separating, distinguishing and sifting pernicious switches and so on.

- **Defense mechanisms based on deployment**
  - Network based
  - Source based
  - Destination based
- **Defense mechanisms based on protocol**
  - TCP
  - IP level defense mechanisms
  - Application level defense mechanisms
- **Defense mechanisms based on time of action**
  - Before the attack
  - After the attack
  - During the attack

## II. MOTIVATION

**Defense components in view of convention (ip based).**

Distinguish and channel parcels with caricature IP addresses at the source's switches in light of the legitimate Ip address extend inner to the system, however the issue is that, the ridiculed bundles won't be identified if the addresses are still in the substantial inward IP address go.

**Network based (D-WARD A Source-End Defense against Flooding Denial-of-Service Attacks)**

Prevent assault movement beginning from a system at the outskirt of the source arrange, however it devours additional memory space as well as CPU cycles than a portion of the system-based guard components.

## III. PROBLEMS IN WIRELESS NETWORK

Serval issues regarding wireless communication are path damage, restricted frequency range, interference, and multipath propagation. Multipath Propagation is, where a signal travels through its starting point to end point, between you will find difficulties that create the signal spread in paths outside the direct line of sight because of reflections, diffraction and refraction along with scattering. Path damage is the weakening of the transmitted signal strength as it circulates away from the sender. Path damage could be driven when the ratio among the powers of the transmitted signal on the receiver signal. This is primarily determined by many factors including the nature and radio frequency of the surface. It is occasionally significant to calculate the path damage in wireless communication networks. Because of the radio frequency as well as the terrain's nature are not identical anywhere, it is difficulty to calculate the path damage throughout message. Throughout communication a quantity of signals in the atmosphere might inhibit with each other causing the damage of the initial signal. Frequency Spectrum is Restricted when frequency bands are used through number of wireless technologies rather than through single wireless technology.

## IV. LITERATURE SURVEY

Classification of attacks

A. Mobile vs. wired attackers:

Mobile attackers have the similar abilities as which of other nodes of specific ad hoc network. Taking the identical source limits, their abilities to damage the networks processes becomes additionally restricted. For example, through the restricted transmitting proficiencies as well as battery powers, mobile attackers might just jam the wireless connections inside its area. They are not able to release the network blocking attacks to interrupt the entire networks activities. Differently, wired attackers are attackers which are able to increasing permission to access the external resources like the electricity. Because they have extra sources, they might release more strict attacks in the networks, like breaking expensive cryptography algorithms or blocking the entire networks. In the ad hoc networks, wired attacker's presence (particularly in the networks which has open environment) is usually possible because the wired attackers are competent to find themselves in the network range and also have a chance to access the supported structures.

B. Passive vs. Active attacks:

Attack classes may consist of communication's passive monitoring, close-in attacks, attacks by the service provider, active network attacks, along with misuse via insiders. Information systems along with networks provides attractive targets along with must become defiant to attack from the complete range of risk agents, from hackers to nation-states. A structure should have the capability to restrict harm as well as improve quickly when attacks happen. In ad hoc networks, attacks are usually classify into 2 groups:

Passive attacks: It include just data's eavesdropping.

Active attacks: It involve activities which are execute by attacker, like deletion, modification as well as replication of communicated data.

1. Passive Attack: Unencrypted traffic is monitored by passive attack and appears for sensitive information as well as clear-text passwords which could be utilized in different kinds of attacks.

Passive attacks comprise information of decrypting weakly encrypted traffic, traffic investigation, insecure communications, and capturing validation data like passwords. Passive interference of network functions allows challengers to detect forthcoming activities. It generates in the discovery of data or information records to an attacker deprived of the user's authorization or awareness.

2. Active Attack: In this, the attacker attempts to avoid or breakdown into protected structures. This could be completed by worms, Trojan horses, viruses or stealth. Attempts are included by active attacks to avert or break safety attributes, to current malicious code, as well as to change or steal data [3].

C. Inside vs. Outside Attacks:

An attacker has cooperated or taken a node, therefore acquisition entry to encryption as well as authentication keys in an insider

attack. The main technique of mitigating as well as detecting insider attacks is to monitoring the package forwarding conduct between the nodes. On the other hand, in an outsider attack, attackers claimed to not have any key's information which are utilized to encode and validation. Avoiding external attacker's interference in the information is attained simply through engaging encryption and validation systems.

D. Layered Attacks:

Attacks could additionally be categorized according to the layer on which the attack occurs, as demonstrated in the table given below:

Table 1 Layer Attacks

| Layers | Attacks |
|---|---|
| Application Layer | Repudiation, Data corruption |
| Transport Layer | Session Hijacking, SYN Flooding |
| Network Layer | Gray Hole, Black Hole, Worm Hole, Byzantine, Sybil, Jellyfish, Rushing |
| Link Layer | Interception, Fabrication, Modification |
| Physical Layer | Jamming, sniffing |

E. Data vs. Control Traffic Attacks:

In data traffic attack either data packets that are being passed through it has been reduced or data packet's forwarding is suspended. Several kinds of attacks select target packages for reducing although few of which drops most of them regardless of sender node. It might extremely reduce the services quality as well as rises EED. This leads to considerable damage of essential data. Whereas, during Control traffic attack, an attacker effort to use to a lawful path through intentionally tampered routing communications. Or on the similar note, attacker initially listen to wireless traffic for control communication after which it generates false package to use the path for the next time when route demand is again directed.

The conventional methods comprise the grade diffusion (GD) [13] algorithm to sensor network routing along with the DD (directed diffusion) [9] algorithm. Such optimizations might ultimately enhances the lifetime of WSN along with diminish sensor node restoration price.

A. Directed Diffusion Algorithm

In recent years, for wireless sensor networks various routing algorithms [10], [14] are suggested. DD algorithm was proposed by C. Intanagonwiwat et al. in 2003 [9]. The Directed Diffusion algorithm's objective is to diminish the counts of information relay transmission for management of power. It is a query-driven transmission procedure. From the sink node, the gathered information is sent just in case its competitions the query. In Directed Diffusion algorithm, queries are offered by sink node in attribute-value pairs to another sensor nodes by spreading the request packages to the entire network. Thus, the information is delivered to the sink node by sensor nodes when queries are matched.

B. Grade Diffusion Algorithm

Grade Diffusion Algorithm was presented by H. C. Shih et al. in 2012 [7] for improving the LD-ACO (ladder diffusion ant colony optimization) algorithm in WSN [6]. This algorithm generates the routing for every sensor node along with that for decreasing the transmission loading neighbor node set is also identified. A sensor node is selected from neighbor node set by every sensor node when node is able to relay as selected by the node's grade table. The Grade Diffusion algorithm also capture data relay information. After that, sensor is able to choose a node that has more accessible energy or lighter loading compared to others to do the additional relay procedure. Furthermore, in real time the routing path is appraised by the Grade Diffusion algorithm as well as the occasion information is therefore transferred correctly and quickly to the sink node. Either the GD or the DD algorithm is utilized, the interested query packages or grade producing packets first be transmission. After that, sink node receives the occasion information as transferred by sensor nodes, based on the algorithm, as appropriate actions happen. The following figure shows the sensor routing paths.

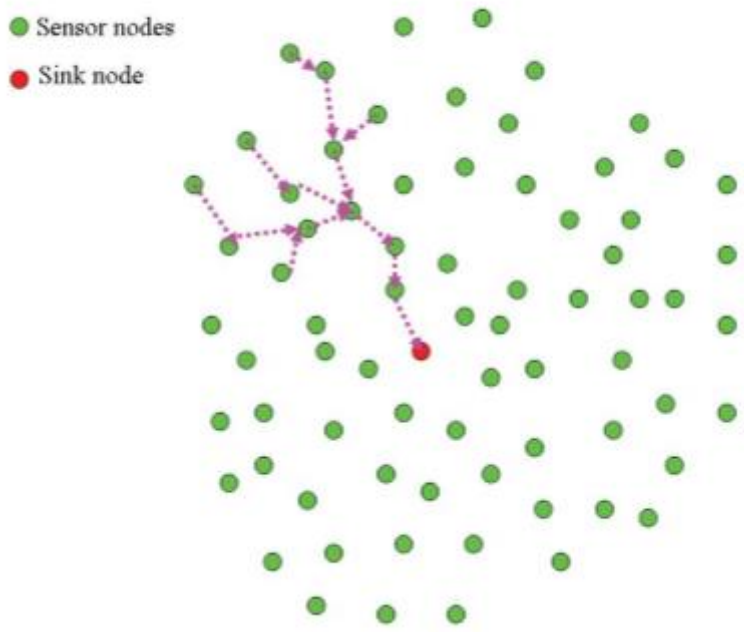


Fig.1 Routing of wireless sensor node

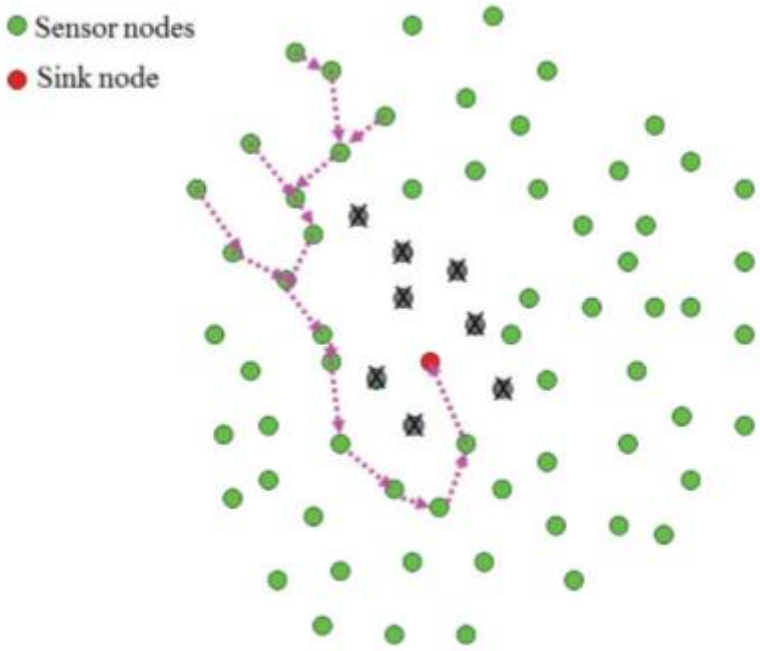


Fig.2 Routing path of wireless sensor node when some nodes are not functioning

**V COMPARATIVE ANALYSIS OF EXISTING SOLUTIONS**

The WSN might fail because of a variety of reasons, which include the following: the nodes wear out after the WSN was in utilize for a long time; the routing path may experience a break; several sensor nodes' batteries get exhausted, needing much more relay nodes; or a leak may be experienced by the WSN sensing area. The state in that the exterior nodes transfers' event information to the sink node through the interior nodes (the sensor nodes close to the sink node) in a WSN demonstrated in figure 2 which shows non-working nodes' accommodation actions. The interior nodes hence have consuming energy at a quicker rate and biggest data transmission loading. If every inside cease to function or reduces their energy, the occasion information could not be routed to the sink node, so there will be no functionality in WSN. In WSN, the power utilization of sensor node cannot be avoided. Furthermore, an algorithm is presented in this paper for finding then change less sensor nodes along with it also to recycle the maximum routing paths. Non-linear functions with several variables cannot be optimized by the traditional search methods. GA (Genetic algorithm) is one system [4], is a directed arbitrary search method established in 1975, according to natural genetics idea. An FNR (fault node recovery) algorithm has been suggested by this paper that according to the GD algorithm collective with the GA. It produces a routing table utilizing the GD algorithm as well as with the GA sensor nodes are changed when ideal sensor nodes surpasses the threshold. This algorithm reuses majority of routing paths for enhancing lifetime of WSN as well as diminishes the replacement price. The MANETs attacks may be characterized as passive or active. Active attacks might be either fixed to interrupt the normal functioning of a particular node or target the functioning of the entire

network. Whereas during passive attacks, no message is transmitted by the attacker, but simply channel is sensed by them. It is non-disruptive but are looking for data that might be vital in the protocol's operation.

The absence of any infrastructure added with the lively topology feature of MANETs make these networks extremely weak to routing attacks such as Flooding, Blackhole, Sybil and so on. In Flooding or Denial of Service (DOS) attacks, a node sends a malicious transmission updating that it has the least path to the destination, through the aim of interrupting messages. In this situation, a malicious node (so-called attacker node) is able to attract each packet by utilizing forged Route Reply packet to wrongly claim that "fake" quickest route to the destination and it removes the packages without forwarding them to the destination.

In DOS attacks, the malicious node is not primarily recognized, for example subsequently it turns malicious just at a later time, avoiding a trust-based security answer from noticing its occurrence in the network. Then collectively forwards/discards the data packets when packet go through it. The malicious nodes are also known as affected/false/fake/abnormal Nodes in this case and there is no alternative mechanisms to resolve the issues related to the routing as well as avoid the attack possibilities while communication.

Table 2. Comparative analysis of different protocols

| | |
|---|---|
| Table-Driven or proactive routing protocols (WRP, CGSR, DSDV, STAR) | Table-Driven or proactive routing protocols. For proactive routing, every node must keep 1 or additional tables to keep routing information, together with any modifications in topology have to be reflected by propagating updates through the network in an effort to have a regular network perspective. |
| Reactive or on-demand routing protocols (DSR, AODV) | Reactive routing is recognized as on-demand routing process because they don't maintain routing information or routing activity in the network nodes when there's no communication. In case a node would like to send a package to another node then this protocol finds for the route in an on-demand way and also establishes the connection to be able to transmit and receive the package. The route find happens by flooding the route request packets through the network. |
| Hybrid routing protocols (ZRF, TORA, OORP, ARPAM) | They present a hybrid design which combines proactive and reactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol which divides the network into zones. ZRP gives a hierarchical structure in which every node has to maintain extra topological information needing additional memory. |

Table 3. Literature review of different papers

| Paper | Advantages | Algorithms Used | Issues Found |
|---|---|---|---|
| [1] | It ensures burst traffic's QoS (Quality of Service). | Period Based Defense Mechanism (PDM) is utilized for improving the burst traffic's throughput. | If the quantity of packages per second is highest (burst traffic), then because of source exhaustion packages cannot be processed by AODV. |
| [2] | The neighbors are characterised into strangers (not trusted), friends (most trusted), along with acquaintances (trusted) in FAP.<br>Thus, it is simply identified. | FAP (Flooding Attack Prevention) was developed, in which FAP states a defense structure against the Ad Hoc Flooding Attack.<br>Intruder's behavior is analyzed and then with help of trust function it is checked. | The issue is it doesn't work correctly with HIGHER NODE MOBILITY. |
| [3] | When flooding packets' quantity is in processing power of NIC, then majority packets in the line are discarded. | The flooding attack impact on the network performance is examined within the conditions of several parameters which include<br>• Network bandwidth<br>• Number of attack nodes<br>• Flooding frequency<br>• Number of normal nodes | If the flooding frequency improves, it results in package delay. Also, packets are damaged with extended routes, on exhaustion of network resources along with growing flooding attacks frequency. |
| [4] | The Accuracy is considered enhanced, resulting in better understanding and forecasting such phenomena. | For hello flood detection, security framework is suggested through<br>A client puzzle technique | In the techniques, sender is treated as attacker if node does not get reply message within specified period. |

| | | | |
|---|---|---|---|
| | | A signal strength technique | |
| [5] | If the node identifies the sender is originating data flooding, it cut off the route and send error message. | The Distributive method was suggested to identify and avoid the RREQ flooding attack. The suggested method's efficiency based on threshold values' choice. | It gets gaps in identify the mischievous node by enabling them to forward much more package till timeout happens. |
| [6] | Data traffic was easily processed by nodes because there is reduction in unnecessary traffic, in this technique. Also, destination node is updated with data in shorter time. | The trust algorithm performance is utilized to assessment the AdHoc network for applying AODV protocol. | This particular effort did not acquire complete model for security attacks along with a reliable security frame-work against ad hoc network's every possible security attacks. |
| [7] | Flexibility is supplied by the algorithm. It is simple to apply with assured message dissemination. | In MANETs, probabilistic flooding algorithm has been recommended by this paper. Rebroadcast probability is regulated by the algorithm through network density consideration. | If the rebroadcast probability p is set to a small value, the reachability would be poor. |
| [8] | To keep high reliability, in order to decrease the broadcast packages quantity. | A purely probabilistic method was discussed regarding flooding, their attempt in exploiting the phenomenon of phase transition. | A system go through certain parameter's tiny change in the device that induced system's global behavior with a great shift. The phenomenon must be very cost effective. |
| [9] | The protocol may be built safe against other kinds of potential DOS attacks as well as none of the real nodes in the network are wrongly accused as misbehaving node. | A simple rate-based control packet forwarding mechanism was introduced to mitigate malicious control package. | This process doesn't capable to differentiate between genuine and forged RREQs from the malicious or victim nodes. |
| [10] | The Mistral compensating mechanism could be useful to other application in which the package damage is a problem. | The Mistral compensating mechanism could support flooding through a wide range of active applications. | It permits just restricted simulation modification and the source code could be estimated with just minor changes. |
| [11] | It could efficiently detect and abolish the nodes which are flooding the network. | ASR (Anonymous Secure Routing) protocol had been considered. It studies how an attacker could severely reduce the network's performance. | In ASR routing protocol, it is not possible to track back the source and destination nodes in an anonymous network. |

**REFERENCES**


[1] Bahaddur, Indira, C. L. Triveni, and P. C. Srikanth. "Novel Defense mechanism against data flooding attacks in ad hoc network." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

[2] Chouhan, Neetu Singh, and Shweta Yadav. "Flooding attacks prevention in MANET." International Journal of Computer Technology and Electronics Engineering (IJCTEE) 1.3 (2011): 2011.

[3] Yi, Ping, et al. "Performance analysis of mobile ad hoc networks under flooding attacks." Journal of Systems Engineering and Electronics 22.2 (2011): 334-339.

[4] Singh, Virendra Pal, Sweta Jain, and Jyoti Singhai. "Hello flood attack and its countermeasures in wireless sensor networks." IJCSI International Journal of Computer Science Issues 7.11 (2010): 23-27.

[5] Shandilya, Shishir K., and Sunita Sahu. "A trust based security scheme for RREQ flooding attack in MANET." International journal of computer applications 5.12 (2010): 4-8.

[6] Performance of AOMDV Routing Protocol Under Rushing and Flooding Attacks in MANET ,2015

[7] SYN FLOODING ATTACK – IDENTIFICATION AND ANALYSIS , 2014

[8] Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol , 2014.

[9] Flooding Attacks Prevention in MANET , 2013

[10] Flooding Attacks Detection in MANETs , 2015

[11] A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks , 2015

[12] A survey defense mechanisms against distributed denial pf service flooding attacks , IEEE 2013.

[13] A Literature Review of Security Attack in Mobile Ad-hoc Networks Nov. 2010.

[14] An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in MANET , 2013.
[15] Detection of Malicious Attack in MANET A Behavioral Approach , 2013.
[16] J. A. Carballido, I. Ponzoni, and N. B. Brignole, "CGD-GA: A graphbased genetic algorithm for sensor network design," Inf. Sci., vol. 177, no. 22, pp. 5091–5102, 2007.
[17] F. C. Chang and H. C. Huang, "A refactoring method for cache-efficient swarm intelligence algorithms," Inf. Sci., vol. 192, no. 1, pp. 39–49, Jun. 2012.
[18] S. Corson and J. Macker, Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. New York, NY, USA: ACM, 1999.
[19] M. Gen and R. Cheng, Genetic Algorithms and Engineering Design. New York, NY, USA: Wiley, 1997.
[20] Z. He, B. S. Lee, and X. S. Wang, "Aggregation in sensor networks with a user-provided quality of service goal," Inf. Sci., vol. 178, no. 9, pp. 2128–2149, 2008.
[21] J. H. Ho, H. C. Shih, B. Y. Liao, and S. C. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks," Inf. Sci., vol. 192, pp. 204–212, Jun. 2012.
[22] J. H. Ho, H. C. Shih, B. Y. Liao, and J. S. Pan, "Grade diffusion algorithm," in Proc. 2nd Int. Conf. Eng. Technol. Innov., 2012, pp. 2064–2068.
[23] T. P. Hong and C. H. Wu, "An improved weighted clustering algorithm for determination of application nodes in heterogeneous sensor networks," J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 173–184, 2011.
[24] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 2–16, Feb. 2003.
[25] W. H. Liao, Y. Kao, and C. M. Fan, "Data aggregation in wireless sensor networks using ant colony algorithm," J. Netw. Comput. Appl., vol. 31, no. 4, pp. 387–401, 2008.
[26] T. H. Liu, S. C. Yi, and X. W. Wang, "A fault management protocol for low-energy and efficient wireless sensor networks," J. Inf. Hiding Multimedia Signal Process., vol. 4, no. 1, pp. 34–45, 2013.
[27] N. Dutta, HKD Sarma and Z. Polkowski, "Cluster based routing in cognitive radio Adhoc networks: reconnoitering SINR and ETT impact on clustering", Com. Com., (Elsevier), pp. 10-20, vol. 115, 2018.
[28] N. Dutta and HKD Sarma, "A probability based stable routing for cognitive radio Adhoc networks", Wire. Net., (Springer), vol. 23(1), pp. 65-78, 2017.
[29] N. Dutta and IS Misra,"Multilayer hierarchical model for mobility management in IPv6: a mathematical exploration", Wire. Pers. Comm.(Springer), vol.78 (2),pp.1413-1439, 2014.
[30] N. Dutta and IS Misra, "Mathematical modelling of HMIPv6 based network architecture in search of an optimal Performance", IEEE 15 th ADCOM, Guwahati, India, pp. 599-605, 2007.