UCR: Unassailable and Coherent Routing view for Aerial Mesh Networks

[1] Ms. Prachi Gurjar, [2] Mrs. Swathi Y

[1]Final Year, M.Tech in Computer Network and Engineering,
[2] Head of the Dept. of Computer Science and Engineering,
[1]CMR Institute of Technology, Bangalore, India

***Abstract*— Mesh networks, embedded with entities such that can wireless, communicating in air "Unmanned Aerial-Vehicle" (UAVs), builds airborne mesh network with WLAN, which incorporates applications such as: As a key significant results in the case just as catastrophic condition, adaptive in different surrounds, decisive and effective gets associated as part in a wider area. Massive accomplishment and tremendous advantages faces provocation in the design of the network as it is vulnerable to security routing attacks, network dereliction forces to lose command over UAVs. Prevention of such vulnerabilities by IEEE 802.11i/s security approach, which would not be sufficient and thus require highly precise secure mechanism for proper deployment of UAV-WMNs. The utilization of cryptographic digital signature combined by ECC and the required appropriate routing protocols gives the necessary protection against the wormhole (external-attack) and blackhole (internal-attacks) in the affected oar intricate in Wireless environment. The UCR approach offers the efficient routing, low anonymity, high cloaked area with lower MBR and mostly the high performance extending the contemporary routing, anonymity issues and its aspects of surveillance to other threats of WMNs, also the collateral approach which when compared to other similar approaches such as PASER and other protocols.**

***Index Terms*— UAV, WMN, ARAN, BATMAN, ECDSA.**

I. Introduction

Multipurpose of the device/equipment is utilized in aerial very-low altitude, is concerned to as- UAV [2], and is, one of the application in this trending technologies. Achievable at very cheaper rates with less cost, also with wider number of benefits. These devices can also be rendered with a variety features (specifications) like it can include number of sensors- which can be of different purpose, wireless transceivers, and positioning capabilities or the operation of it.

Knowing the increasing rate of disasters leads in intense economic damage and disruption of telecommunications. These are the facets which manifests, highly focus on (portable or mobile features) interaction case of disasters, shows the communication network which do not rely/depend on current infrastructure and can be deployed in a very short period/ duration example: an hour. The solution to overcome the above crisis is the use of Low altitude UAV's, as aerial WLAN hotspots. The application of this UAV in extensive area, forged specifically. Implementing highly impeccable, automated and self-repairing; wireless network is required to connect to the aerial vehicle, cellular network and internet at ground station.

WMNs [3], are the affirmative, as they have aforementioned characteristics, and they offer a wide physical air-link (air-to-air) for a direct interaction between the UAVs, and specified network is called as an UAV-WMN in the whole project. As WMNs are dynamic (mobile) by nature, i.e., Inclines the topology, because in the changing time, since the addition or removal of a node with the combination or by the result of the change in the network environment and also, since the mobility of the entities. The topology of an UAV-WMN is highly dynamic no doubt for it is a typical mobile network.

AODV protocol, entrenches for paths to destination whenever desired (on demand). The hop counts (also sequence-numbers) with added time-out, included for avoidance of routing-loops thus controls only active routes. The basic mechanism here is request-reply for route discovery. With the associated unique feature of sequence- numbers, the detection of outdated data (for current route) and information of route. HELLO message, helps for information connectivity to find for breakage of links and error messages on active routes. This safeguards/protects with offering the flexibility of routing loops and prevents the issues (which is called as "count to infinity").

An Asymmetric algorithm, where the secrecy is preserved is ECDSA. It is carried on, with what is called as secret key idea for which the participants possess both public key as well the private key (use to sign the message to be sent) of its own, and the destination participant verifies. Thus, this method is accepted by "NIST" for "DS" Standards thus resulting for the suitable "ECDSA" used. Some of the unique properties of it are assurance of data, it is non repudiation, provides two times security for the purpose of the information exchange.

II. BACKGROUND AND RELATED WORK

A. Issues in WMNs

In the case, when intricacy in WMNs influences some insider and external attacks, which introduce adverse effect on performance and service of network.

1. In external attack, the unauthorized user who snoops the packets and also respond back to it, further proceeds by capturing the network resources eventually. When attacker traces all the messages (Time-based replay) or routes (Position-based replay) of nodes and sends it back after some interval. A compound attack, which integrates these attacks by forming a tunnel (path) between nodes and forwards the packets to distant node as the next neighbor node.
2. The nodes in the network which acts as the legitimate nodes, access all credentials for its services and instead of forwarding the messages. This is found in the internal attacks, it drops, example: repeatedly broadcasting request messages (Flooding), fraudulent identity of nodes (IP spoofing), changing the destination and sequence- number (Blackhole attack).

These issue makes it very hard for the WMN to be command and have UAV's in leash, operated remotely and controlled by a ground station. UAV depends on the exchange of information from ACP (autonomous cooperative positioning) which will make it easy for the attacker to change the coordinates of the UAV by secretively dropping data packets.

In some cases, there is no way to effectively refreshes the credentials of it, for the attacker may (or will be) be able to alter or modify or even change the network credentials and change the data packets or inject corrupted information of control which could be hijack the UAV, which is illegal. For instance, the UAV might be impersonated by the attacker and dispatch corrupted information about the position, revealing the collision avoidance mechanisms of the UAV to steer indirectly its direction to the area controlled by the attacker. Since the breaching done while the entities' interaction of the security system of the flight/UAV can lead to fatal risks or consequences, therefore it is necessary to dispatch a secure UAV-WMN backbone. Different layers of WMN stack have indefinite vulnerabilities, these weaken and muddle the network.

B. Contributions

Numerous researches and experiments were proposed to deal with the above issues of security in mesh communication. So many such protocols and security mechanism were applied to mitigate the vulnerability and reach the expected optimization.

ARAN [4]: is such an example which is used for ad hoc networks, spotted and secured/protected against malevolent alacrity and also the routing attacks. In addition to this, the DOS based on the mechanism of message dropping, flooding and the resource mitigation in the network; is all focused on by this protocol. It follows the redirection method through modification of attacks: that is by transforming the sequence-number by using the AODV and DSDV, also the hop counts, route and tunneling.

BATMANs: for mesh networks usually used for small campus that is in one roof itself. Works in 2 layer routing, checked for performance and reachability. It need not refer to OLSR and thus works better scalable than OLSR, preferred for dynamic network.

HWMP: is the transforming of AODV, radio wave link metrics and MAC address and thus is use for path assortment process.

PASER [1]: Uses the key transient (in MAC), uses Merkle tree (token mechanism). As it uses KDC for switch-over, all the entities will share the same key (group-key management) which tends the attacker to grab the censored data with ease by trying out all the possibility patterns to decrypt the key. Suspended to buffer overflow since every transaction the key generated is saved in the memory of the network. Thus every time it fills the memory causing the buffer overflow leads to less storage of data. Having such flaws the need for enhanced new improved protocol is must.

C. Disadvantage of Existing system

All these mentioned existing systems are very much exposed to attacks like blackhole and wormhole. BATMAN captures/picks extremely less amount of information. In spite of all these flaws, the user will lose his/ her privacy, data and thus faces a high risk. The delay caused due to the critical complexities in the network regardless of tremendous efforts by the professionals. Hovering need for better protocol when compared to existing is crucial.

III. PROPOSED SYSTEM

UCR approach aims for attainable routing for the UAV in WMNs with unsusceptible to outbreaks. While to the prior works possessed the weaknesses and pitfalls, which are thus strenuous on with the proposed UCR approach.

A. AODV protocol

Demand-driven protocols, anticipated only when a route to destination is not acknowledged. Where every node bears a table (route table) which is helpful for obtaining the information to the destination. X (source node), announces for the perfect route to the Y (destination node) with a message request (RREQ) all over the network. Along with it flags (several) and a RREQ involves the hopcount, RREQ-identifier, address and sequence-number of the originator and destination.

Of the receipt, the envelope, destination node, route to the aforementioned hop to check if the REQ already received. It abandons the packet if YES, incrementing hop-count by 1 and thus propels the RREP (route reply) to the source node X, in case for communication.

For trial, the broken link, the need for route preservation is must, which follows 2 processes: Firstly, use of the sporadic HELLO message for every 1 hop neighbor if random node doesn't receive within hello-interval time then, it approves for splintering of link. Secondly, by link layer feedback course. In which it allows the quick reaction for when the link breaks (active data transmission) detects if no acknowledgement is received. ERR or RERR message is Then broadcast over all the network includes information of unapproachable next-nodes and also all other unapproachable next-nodes and also of unapproachable nodes. This way the efficient for topology awareness than flooding. It confiscates the destinations than entail the RERR while the next hop from the list.

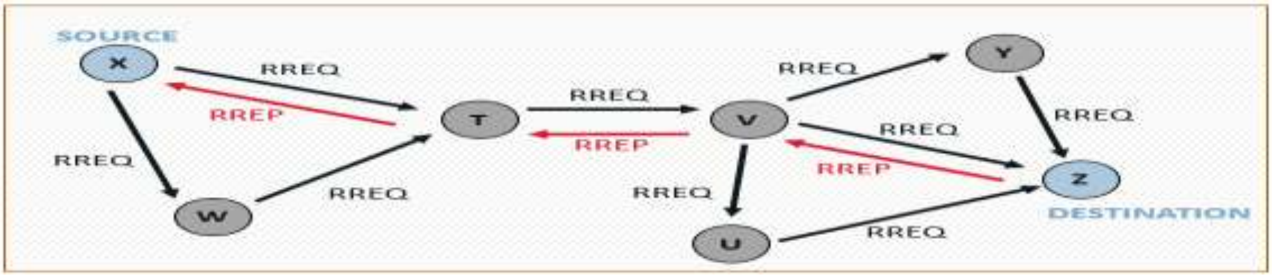


FIG 3.1 Ad-Hoc on-Demand Vector Routing Protocol

B. Elliptic Curve Digital Signature

It comprehends for the asymmetric systems, comprising the private key in the source entity and the public key at the destination. This is mandatory for it to verify the source entity. When in the case where a new entity has to be verified this endorsement of system is very much feasible.

The mechanism of ECDSA [5] is as follows: The key pair cohort (public, private key) followed by signature and the verification.

1. *Key Generation:*

Initially the source entity should know its private key. With the help of private key and domain parameters, the domain parameters. Private Key is retained censored, but the public key is made exposed for any entity to access. The figure demonstrates the key generation process, FIG 3.2.

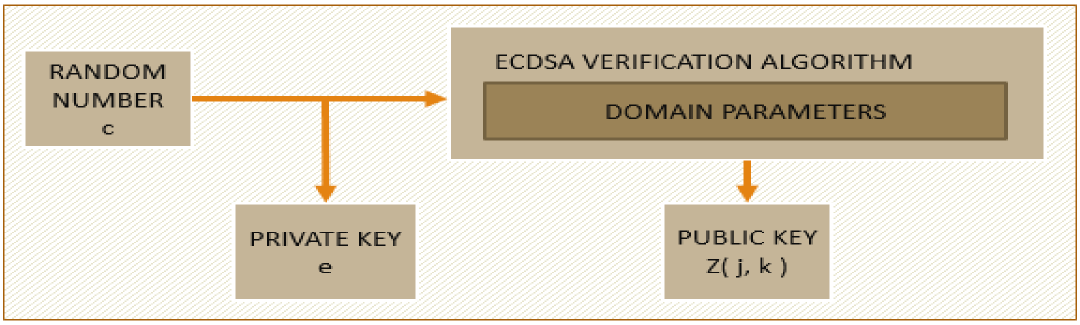


FIG 3.2 Key pair generation process

At the twitch the random number is initiated, while the course terminates. This number is considered as the private key e, which is a scalar. Thus public key Z (j, k) found by,

$$Z\ (j,\ k) = c^*\ T\ (j,\ k) \qquad (3.1)$$

2. *Signature Generation:*

The destination entity can confirms for the message genuineness with the aid of the source entity's public key. The hash algorithm aids to transfigure the variable length to a fixed length of the message digest h (p). Where p is the packet/message. Few distinctive properties of the hash for security are:

- Inevitable: It is very flexible and the message is obtained with ease.
- Destruction hindrance: Cannot find multiple messages.
- Barrage effect: If there is any change in the message, it directly affects the digest.

Thus by this, assessed message digest is to generate a random number to bestow an elliptic curve to calculate the value c, shown in the figure, FIG 3.3.

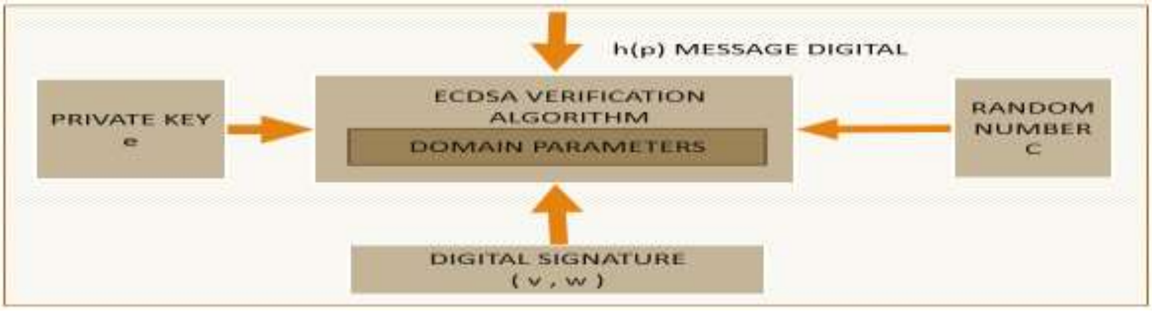


FIG 3.3 Signature Generation process

In this method, the signature obtained will have two (integer) numbers (v, w). Here v is the combination of c and the T (j, k) (basepoint) given as,

$$(j1,\ k1) = c^*\ T\ (j,\ k) \bmod f \qquad (3.2)$$

$$v = j1 \bmod n \qquad (3.3)$$

Whereas, combining all the following parameters such as: h (p), e (private key) and c (random number) can be equated as,

$$w = c^{-1} (h (p) + e * v)) \bmod n \qquad (3.4)$$

3. *Signature Verification:*

This is associated for the signature estimation, where in, by applying the source's public key message digest signed by the source, integrated with Z (j, k) (public key), v and w (components of digital signature) and T (j, k) (basepoints), this is given by,

$$g = w^{-1} \bmod n \qquad (3.5)$$

$$r1 = (h (p) * y) \bmod n \qquad (3.6)$$

$$r2 = (v * y) \bmod n \qquad (3.7)$$

$$(r2, s2) = (((r1 * T (j, k)) + (r2 *Z (j, k))) \bmod n) \qquad (3.8)$$

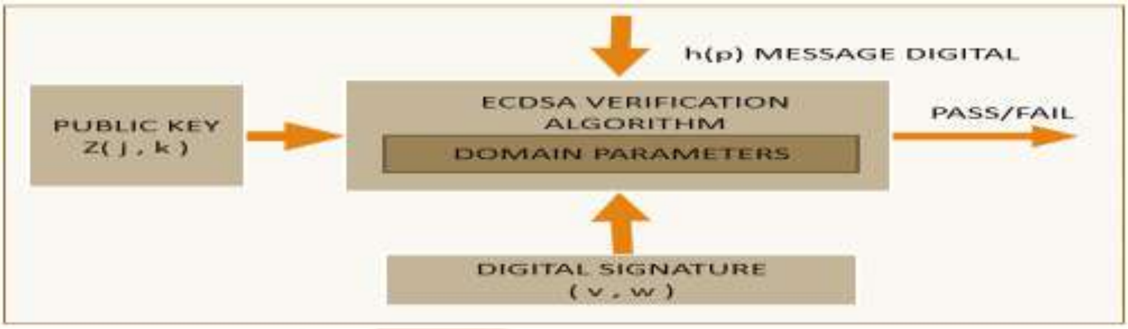


FIG 3.3 Signature Verification process

Thus if verification is successful then it passes, if r2 is equal to v, confirming that signature was rightly computed by using private key.

C. Overview of UCR Architecture

For aerial mesh networks to be implemented, there are few restraints to be monitored in erstwhile. The secure approach, integrity of data, routing coherence, reliability and so on.

Thus the UCR mainly concentrates the basic requirements for the communication in the mesh networks, since seen that the incursion occurs in WMNs with ease, for its unique and dynamic characteristics. Thus considering the pitfalls seen in the previous protocols, the proposed system that is UCR system follows certain criteria, FIG 3.4:

- Incorporates the norms and designs a new model, FIG-3.4, is simple but provides the essential authentication for each and every entity in the network during the formation, as shown in the figure.
- UCR approach is referred as Unassailable and Coherent Routing Protocol, which is implemented with the Adhoc On-demand vector (AODV) protocol for the efficient, reliable routing which is done by on demand protocol. Every requested route entities in update their table accordingly and thus every-time demanded the table is refreshed with the new sequence numbers and the location.
- Security is handled by the ECDSA algorithm. Shared key mechanism is used with the origin entity signs the message to be sent and thus the recipient verifies it. If it is not verified then the message fails.
- Security is handled by the ECDSA algorithm. Shared key mechanism is used with the origin entity signs the message to be sent and thus the recipient verifies it. If it is not verified then the message fails.

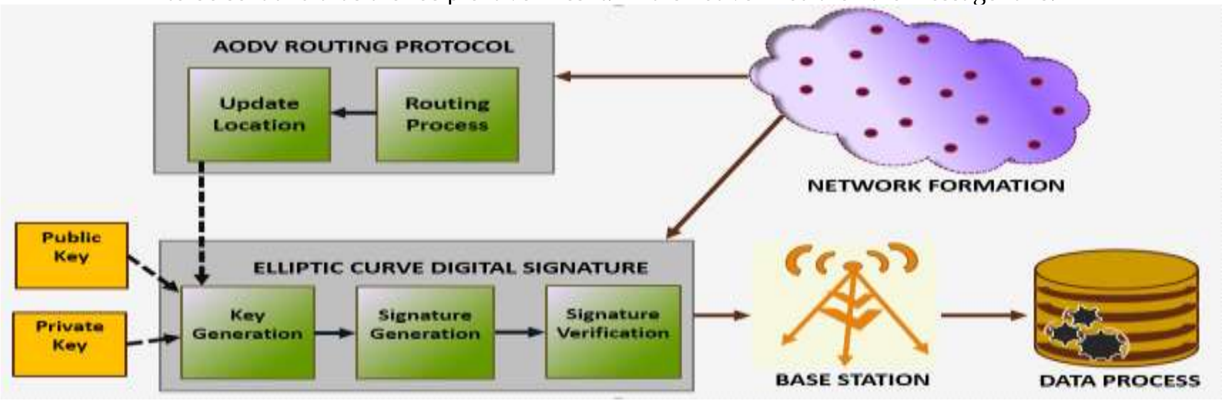


FIG 3.4 UCR, Architecture Diagram

D. UCR Building Blocks

UCR protocol incorporates three basic processes FIG 3.5

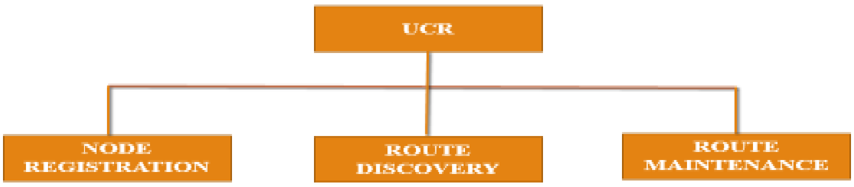


FIG 3.5 UCR, Basic Processes

1) The entity register process, where in the formation of the network every node/entity is registered and then allowed for the communication. This is done by the ECDSA for key generation and authentication. Shared key is imparted between every two nodes collaborating and thus this key will not be exploited by any other two entities desiring to communicate. Those two entity when ready to transfer and receive will generate a shared key for itself. This process includes the signing of the message to be sent to the destination, done by the source entity with the help of the private and its public key using the “elliptic curve DSA” (cryptographic) algorithm.

2) The route sighting, done by the most suitable protocol AODV.

3) The route maintenance, done by the AODV algorithm by updating the route table and thus sends a HELLO message to every other entity to check for an error or mending of link or any other cause.

The communication amongst two entities, here denoted to as UAVs is portrayed in the figure, FIG 3.6. This diagram explains with reference to the process involved by every entity in the system. Node A and Node B are suppose the aerial devices, the registration of both will be initially done in the network and thus the process proceeded.

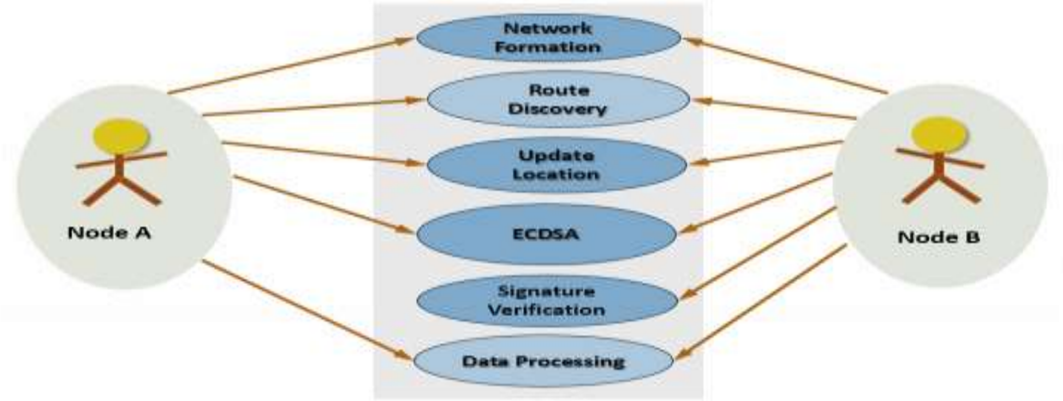


FIG 3.6 UCR, Use-case Diagram

E. UCR Dataflow diagram representation

The data-flow diagram illustrates the entire flow of the system in dispensed fashion, so that the considerate the flow of the system will be at affluence.

The following diagram shows the UCR dataflow in a systematic manner. It consist of three levels. Level 0: Involves the network formation node registration and verification for the data transfer by the two communicating nodes in that same network. The route creation is also done by RREQ broadcast method. Level 1: The table updating done by the nodes in the active network helps to generate the keys and thus the shared key is generated between two communicating nodes. During the message transfer, the ECDSA is implemented for signing the message as well the verification of it. Level 2: Signature verified node is then tested for authentication in the Base station and thus carry on for the data process.

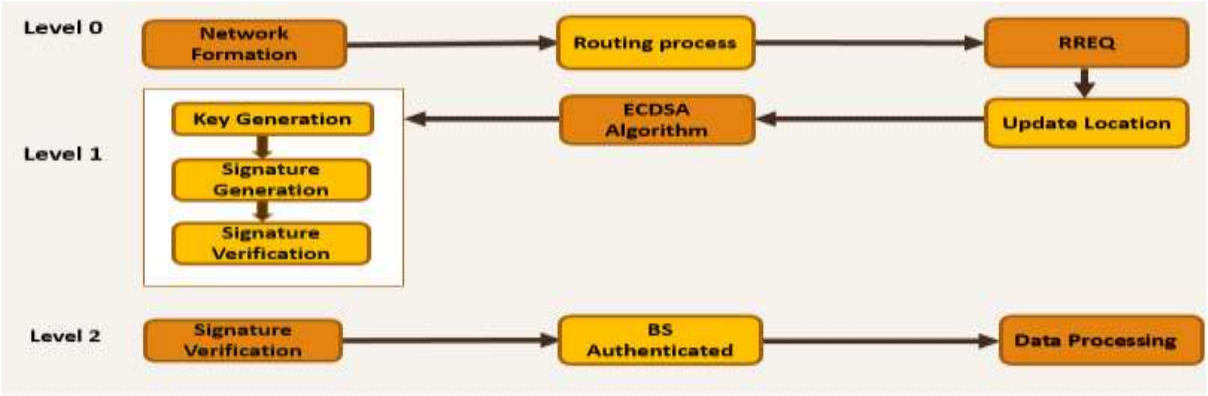


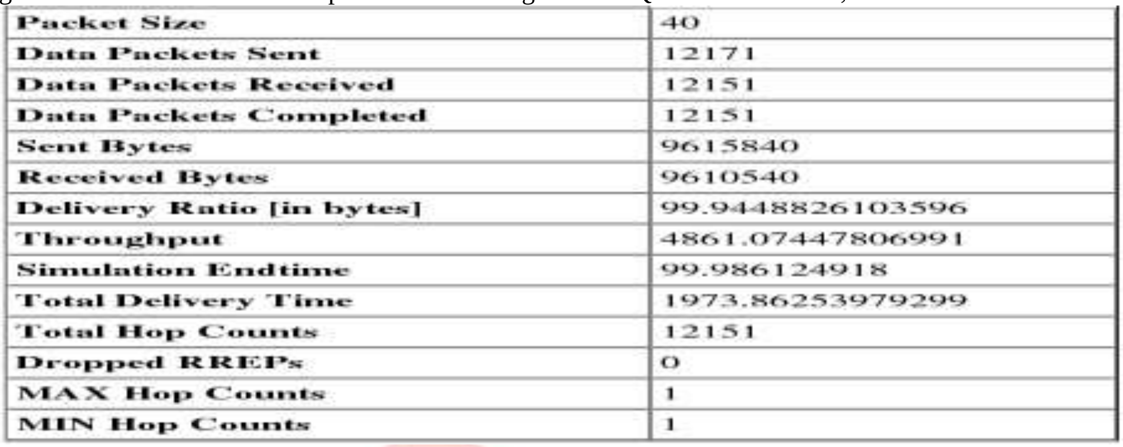
FIG 3.7 UCR, Data-flow diagram

IV. SIMULATION AND RESULTS

A. Simulation evaluation

The anonymity of the UCR is analyzed by modifying the existing approaches to highly secured approach. Particularly the size of each routing table is increased. Here, appliance the UCR, the tool used is Network Simulator 2, version 2.34. This Network Simulator is used for the reason that the network highly realistic with random mobile nodes.

The UCR is evaluated by comparing it to the existing system, the performance is measured and along with the following metrics: 1) Anonymity: This is unsecured level in the system. 2) Estimation rate: The time taken for authentication and verification of nodes. 3) Quarry region size answer error: The response after sending the RREQ to entire network, is not obtained after a certain period. .



Packet Size	40
Data Packets Sent	12171
Data Packets Received	12151
Data Packets Completed	12151
Sent Bytes	9615840
Received Bytes	9610540
Delivery Ratio [in bytes]	99.9448826103596
Throughput	4861.07447806991
Simulation Endtime	99.986124918
Total Delivery Time	1973.86253979299
Total Hop Counts	12151
Dropped RREPs	0
MAX Hop Counts	1
MIN Hop Counts	1

FIG 4.1 Network Simulator Parameters

B. Simulation results

The performance and the other factors of UCR is shown in the figures. FIG 4.2, represents the anonymity level v/s Number of bytes. That is it illustrates the unsecured level in the proposed UCR when compared to the existing system. For existing system it is high, with number of bytes 12 bytes and from typical to drastic escalation of the anonymity level. In contrast, it is in between 2 bytes - 4 bytes and anonymity level is constant at some level.

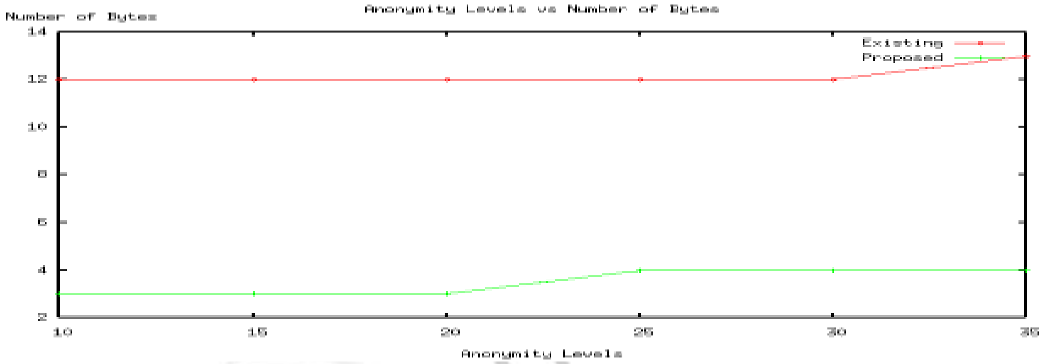


FIG 4.2 Anonymity Level v/s No of Bytes

FIG 4.3 Simulation time Computational Cost graph represents the time taken for authentication of keys and verification. In existing it takes no time to authenticate since it uses group key and thus same key is use for every other communication; 0 computational cost to 13 with respect to Simulation time. The UCR approach is initially 7 to 14 computational cost, with respect to Simulation time, since it uses the two way verification of the key, it takes time for computation.

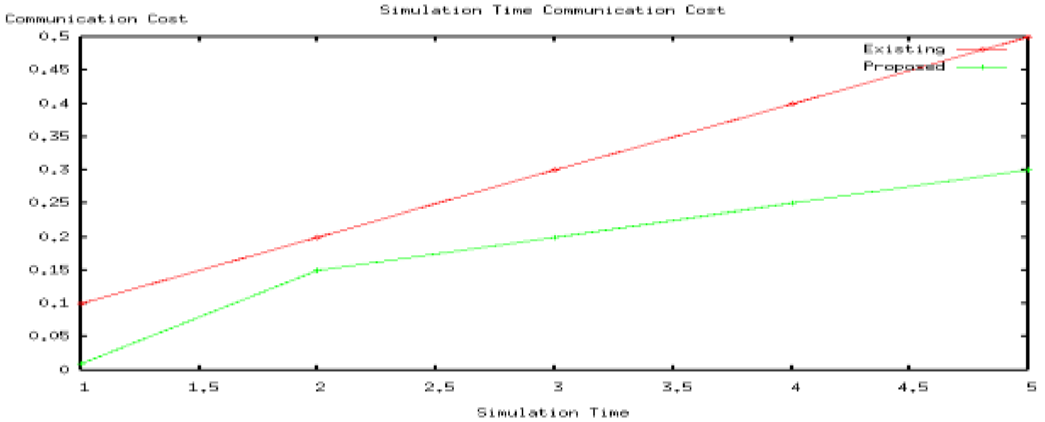


FIG 4.3 Simulation time Computational Cost

FIG 4.4, illustrates the quarry region size answer for error, existing system takes high time to respond back the RERR message when node error occurs, 0.1 Answer error to 0.6 with respect to region size. In UCR, the quarry answer error is less, from 0- 0.1 quarry answer error with respect to region size

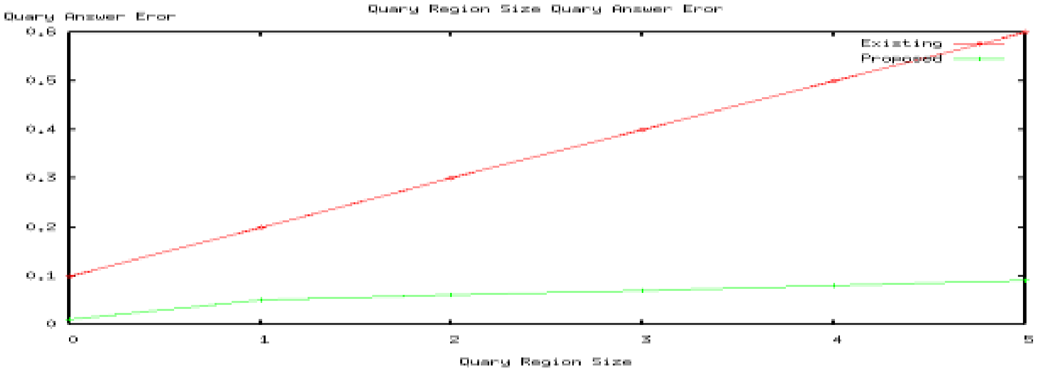


FIG 4.3 Simulation time Computational Cost

V. CONCLUSION

UCR, is a coherent approach which give the maximum performance with the secured mesh route discovery. The protocol is explored with some of other protocols like ARAN, BATMAN and PASER in different scenarios and under various network attacks. Thus the consequence of the UCR shows high tradeoff between security and performance and also maintenance. In contradiction to the other protocols, to protect the network against routing attacks, simultaneously accomplishing a comparable performance with those protocols. The UCR, completely concentrates on the shared key with digital signed message for authentication and verification including the route maintenance. Apart from that, we are extending the wormhole protection of PASER for indoor scenarios using a novel virtual localization technique. The UCR, thus shows the high rate in computational mechanism and has high cloaked area. Whereas when compared to existing system, the MBR rate is less than existing system.

Future work: intend to formally confirm that the security of existing system to provable security. Besides, it aims at analyzing the energy consumption imposed by PASER especially by the GPS component it incorporates. Future work here can also be achieved to obtain considerable method which checks, identifies and exposes the nodes to search the routes and do not forward packets. This work can merge with

REFERENCES

[1] Ajit N Pawar,” Position Aware Secure Routing Using Mesh Network in WNS,” International Journal of Innovative Research in Computer and Communication Engineering vol-4, Issue 12, December 2016.

[2] P.-B. Boek, K. Kohls, D. Behnke, and C. Wietfeld, “Distributed Flow Permission Inspection for Mission-Critical Communication of Untrusted Autonomous Vehicles,” IEEE VTC-2014

[3] R. Matam and S. Tripathy, “Provably Secure Routing Protocol for Wireless Mesh Networks,” Int. Journal of Network Security, vol. 16-2014.

[4] S K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, “Authenticated Routing for Ad hoc Networks,” IEEE Journal on Selected Areas in Communications, vol. 23, 2005

[5] Aqeel Khalique, Kuldip Singh and Sandeep Sood,” Implementation of Curve Digital Signature Algorithm”, Int. Journal of Computer Applications, vol-2, No-2.