IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Efficient Implementation of Active Routing in Wireless Sensor Networks using Random multipath Routes

J. Thirupathi [1], Assoc. Prof. Dept of Computer Science and Engineering, Samara University
K. Ramakrishna[2], Asst .Prof. Dept of Computer Science and Engineering, Samara University

Abstract— Now-a-days security is one of the major issues of data communication over wired and wireless networks. To enhance the security of data transmission, existing system works on the cryptography based algorithms such as SSL, IPSec. Although IPSec and SSL accounts for great level of security, they introduce overheads. A mass of control messages exchanging also needed in order to adopt multiple path deliveries from source to destination now apart from that the proposed dynamic routing algorithm called improved Active Routing in Wireless Sensor Networks using Random multipath Routes. Without introducing extra control messages, the algorithm is implemented and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks.
This routing protocol is compatible with the Routing Information Protocol which uses hop-count as its Routing metric. So there will be a limited number of hops and data transmissions are done by selecting hops randomly in a network. This improves security as well as controls traffic in the network. So, the procedure also includes using the multipath routing to select the paths to be followed. It uses the randomization process for selecting the number of hops to be selected for transforming the data actively. A clear study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the results and to show the capability of the proposed algorithm.

Keywords: **Dynamic routing, Routing information protocol and Distance vector protocol, randomized selector.**

1. INTRODUCTION

Wireless sensor networks (WSNs) have drawn a lot of attention recently due to their broad applications in both military and civilian operations. A WSN usually consists of a large number of ultra small, low-cost devices that have limited energy resources, computation, memory, and communication
capacities and for the applications such as battlefield reconnaissance and homeland security monitoring. WSNs are often deployed in a vast terrain to detect events of interest and deliver data reports over multihop wireless paths to the sink. Data security is essential for these mission critical applications to work in unattended and even hostile environment. Most of the security threats in WSNs are compromised node (CN) and denial of service (DOS). Compromised node (CN) could have multiple nodes to obtain their carried keying materials and control them, and thus is able to intercept data transmitted

through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes and compromised nodes through malicious crypto analysis. Hence, this type of attacks could lead to data confidentiality in WSNs. denial of service (DOS) attack is any event that diminishes or eliminates a network's capacity to perform its expected function Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS. Although attackers commonly use the Internet to exploit software bugs when making DoS attacks. These two WSNs attacks are similar in generating black holes. A black hole is 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. In compromised node, the adversary can always acquire the encryption/decryption Keys of that node, and thus can intercept any information passed through it. Likewise, an adversary can always perform DOS attacks (e.g., jamming) even if it does not have any knowledge of the underlying cryptosystem. WSNs first the packet is broken into P shares using a(K,P) threshold secret sharing mechanism such as the Shamir's algorithm.
The original information can be recovered from a combination of at least T shares, but no information can be guessed from less than P shares. Second, multiple routes from the source to the destination are computed according to some multipath routing algorithm. These routes are node-disjoint or maximally node-disjoint subject to certain constraints (e.g., in-hop routes). The P shares are then distributed over these routes and delivered to the destination. As long as at least P-k+1 (or P) shares bypass the compromised nodes, the adversary cannot acquire the original packet.
In this paper, we propose a active multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are computed in a active way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination, which is practically not possible.
The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets. The proposed algorithm should be easy to implement and compatible with popular routing protocols, such as the

ISSN 2348 – 7968

Routing Information Protocol (RIP) for wired networks [16] and Destination- Sequenced Distance Vector (DSDV) protocol for wireless networks [20], over existing infrastructures. These protocols shall not increase the number of control messages if the proposed algorithm is adopted. An analytic study will be presented for the proposed routing algorithm, and a series of simulation study will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

The proposed algorithm implement's popular routing proto-cols, such as

1. Routing Information Protocol (RIP) for wired networks
2. Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks.

• Those based on RIP, each node maintains a routing table.

• If the proposed algorithm is implemented over RIP with equal cost links, then the Resulted path set would be the same as that generated by an equal-cost multipath protocol based on RIP.

II. LITERATURE SURVEY

A. Data Transmission

Data transmission, digital transmission or digital communications is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint transmission medium. Examples of such media are copper wires, optical fibers, wireless communication media, and storage media. The data is often represented as an electro-magnetic signal, such as an electrical voltage signal, a radio wave or microwave signal or an infra-red signal. While analog communications represents a continuously varying signal, a digital transmission can be broken down into discrete messages. The messages are either represented by a sequence of pulses by means of a line code (base band transmission), or by a limited set of analogue wave forms (pass band transmission), using a digital modulation method. According to the most common definition of digital signal, both baseband and pass band signals representing bit-streams are considered as digital transmission, while an alternative definition only considers the baseband signal as digital, and the pass band transmission as a form of digital-to-analog conversion.

Data transmitted may be digital messages originating from a data source, for example a computer or a keyboard. It may also be an analog signal such as a phone call or a video signal, digitized into a bit-stream for example using pulse-code modulation (PCM) or more advanced source coding (data compression) schemes. This source coding and decoding is carried out by codec equipment.

B. Adaptive routing

Adaptive routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change. People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination. The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. There are several protocols used to achieve this:

• RIP

• OSPF

Systems that do not implement adaptive routing are described as using static routing, where routes through a network are described by fixed paths (statically). A change, such as the loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

C. Routing Information Protocol

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, however, they are considered technically obsolete by more advanced techniques, Open Shortest Path First (OSPF) and the OSI protocol IS-IS. RIP has also been adapted for use in IPv6 networks, a standard known as RIPng.

D. Destination-Sequenced Distance Vector routing

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the Routing Loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. Bellman-Ford algorithm computes single source shortest paths in a weighted digraph. For graphs

with only non-negative edge weights, the faster Dijkstra's algorithm also gives solution to the problem. Thus, Bellman–Ford is used for graphs with negative edge weights. Bellman–Ford's basic structure is very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes all the edges, and does this $|V| - 1$ times, where $|V|$ is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles, the shortest path can only visit each node at most once. Unlike the greedy approach, which

depends on some specific structural assumptions derived from positive weights, this straightforward approach extends to the general case. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently.

ISSN 2348 – 7968

E. Selection of Route

If a router receives new information, then it uses the latest sequence number. If the sequence number is the same as the one already in the table, the route with the better metric is used. Stale entries are those entries that have not been updated for a while. Such entries as well as the routes using those nodes as next hops are deleted.

- *Advantage*

DSDV was one of the early algorithms available. It is quite suitable for creating ad hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm. Many improved forms of this algorithm have been suggested.

F. Multipath routing

Current routing schemes typically focus on discovering a single "optimal" path for routing, according to some desired metric. Accordingly, traffic is always routed over a single path, which often results in substantial waste of network resources. Multipath Routing is an alternative approach that distributes the traffic among several "good paths instead of routing all traffic along a single "best" path. Equal-cost multi-path (ECMP) is a routing technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet the router must decide which next-hop (path) to use.

G. Analysis of an Equal-Cost Multi-Path Algorithm

Equal-cost multi-path routing (ECMP) is a routing strategy where next hop packet forwarding to a single destination can occur over multiple “best paths” which tie for top place in routing metric calculations. Multipath routing can be used in conjunction with most routing protocols, since it is a per-hop decision that is limited to a single router. It potentially offers substantial increases in bandwidth by load-balancing traffic over multiple paths. However, there can be significant problems in its deployment in practice. Load balancing by per-packet multipath routing is generally deprecated due to the impact of rapidly changing latency, packet reordering and
maximum transmission unit (MTU) differences within a network flow, which can disrupt the operation of many Internet protocols, most notably TCP and path MTU discovery. In many situations, ECMP may not offer any real advantage over best-path routing: for example, if the multiple best next-hop paths to a destination reconverge
downstream into a single low-bandwidth path (a common scenario), it will merely add complexity to the traffic paths to that destination without improving available bandwidth.

In many situations, ECMP may not offer any real advantage over best-path routing: for example, if the multiple best next-hop paths to a destination reconverge
downstream into a single low-bandwidth path (a common scenario), it will merely add complexity to the traffic paths to that destination without improving available bandwidth. ECMP may also interact negatively with other routing algorithms where the physical topology of the system differs from the logical topology, for example in systems that employ VLANs at layer 2, or virtual circuit-based architectures such as ATM or MPLS. Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multi-path routing techniques, but multi-path routing is not yet widely deployed in practice.

H Equal Cost Load Balancing

You may be wondering what happens if a routing table has two or more paths with the same metric to the same destination network. When a router has multiple paths to a destination network and the value of that metric (hop count, bandwidth, etc.) is the same, this is known as an
equal cost metric, and the router will perform equal cost load balancing. The routing table will contain the single destination network but will have multiple exit interfaces, one for each equal cost path. The router will forward packets using the multiple exit interfaces listed in the routing table.

Destination Node(t)	Cost($W_{Ni,,t}$)	Nexthop
N1	9	N6

Destin-ation Node(t)	Cost(wNi,t)	Nexthop Candidates (CNi)	History Record for Packet Deliveries to The Destination Node t(H_{Ni}) t
N1	9	{N6,N21,N9}	{(N_2, N_{21}),(N_3, N_6),…,(N_{31}, N_{20})}
N2	10	{ N9, N21}	{(N_1, N_9),(N_3, N_9),…,(N_{31}, N_{21})}
N3	11	{ N9}	{(N_1, N_9),(N_2, N_9),…,(N_{31}, N_9)}
N2	10	N21	
N3	11	N9	

The routing table for the original distance-vector-based routing algorithm

The routing table for the proposed security enhanced routing Algorithm

3 RANDOMIZATION PROCESS

Consider the delivery of a packet with the destination t at a node Ni. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries shown in Procedure 1 is adopted. In this process, the previous nexthop hs (defined in of Table 1b) for the source node s is identified in the first step of the process (line 1). Then, the process randomly picks up a neighbouring node in excluding h_s as the nexthop for the current packet transmission. The exclusion of h_s for the nexthop selection avoids transmit-

ting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

RANDOMIZED SELECTOR (s, t, pkt)
1: Let hs be the used nexthop for the delivery for the source node s.
2: if hs Є C_{tNi} then
3: if | C_{tNi} |> 1 then
4: Randomly choose a node x from { C_{tNi} -hs } as a nexthop, and send the packet pkt to the node x.
5: h_s ← x, and update the routing table of Ni.
6: else
7: Send the packet pkt to hs.
8: end if
9: else
10: Randomly choose a node y from CtNi as a nexthop, and send the packet pkt to the node y.
11: hs ← y, and update the routing table of Ni.
12: end if

E. Routing Table Maintenance

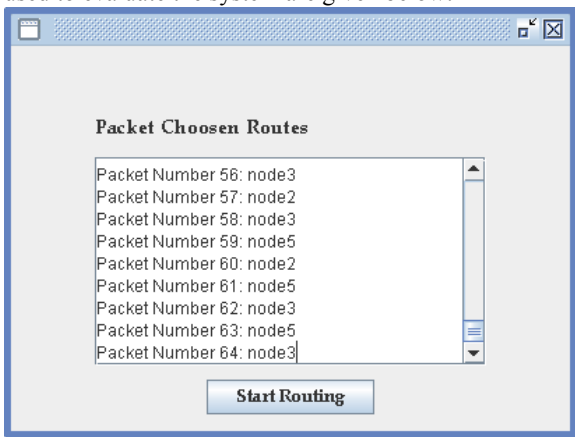
Let every node in the network be given a routing table and a link table. We assume that the link table of each node is constructed by an existing link discovery protocol, such as the Hello protocol.

DVPROCESS(t,WNj,t)
1: if the destination node t is not in the routing table then
2: Add the entry (t,($w_{Ni,Nj}$ +W_{Njt}), $C_{Ni,t}$={Nj};H_{Nit} =Ø)
3: else if ($W_{Ni;Nj}$ +$W_{Nj,t}$)<$W_{Ni,t}$ then
4: C_{Nit}←{Nj} and Nj is marked as the minimal-cost nexthop.
5: $W_{Ni,t}$ ←($W_{Ni,Nj}$ +WNj,t)
6: for each node N_k <Nbr_i except Nj do
7: if $W_{Nk,t}$ <WNi,t then
8: C_{Nit} ←CNi.t U{Nk}
9: end if
10: end for
11: Send (t,$W_{Ni,t}$) to each neighboring node Nk ЄNbr_i.
12: else if ($w_{Ni,Nj}$ + $W_{Nj,t}$)>$W_{Ni,t}$ then
13: if (Nj Є CNi ,t) then
14: if Nj was marked as the minimal-cost nexthop then
15: WNi,t ←MINNkЄNbr,i (WN,,Nk +WNk,t)
16: CNit ←Ø
17: for each node Nk ЄNbri do
18: if $W_{Nk,t}$ <$W_{Ni,t}$ then
19: CNi←t U {Nk}
20: end if
21: end for
22: Send (t,$W_{Ni,t}$) to each neighboring node N_k Є Nbr_i.
23: else if $W_{Nj,t}$ >$W_{Ni,t}$ then
24: C_{Nit}←CNi-{N_j}
25: end if
26: else if (Nj Є C_{Nit})^ ($W_{Nj,t}$ <$W_{Ni,t}$)then
27: C_{Nit} ←C_{Nit} U {Nj}
28: end if
29: end if

Initially, the routing table of each node (e.g., the node N_i) consists of entries {(N_j, wN_i,N_j , C_{NjNi}={Nj}, H_{NjNi}=ø},where N_j Є Nbr_i and wN_i,N_j = wN_i,N_j. By exchanging distance vectors between neighbouring nodes, the routing table of Ni is accordingly updated. Note that the exchanging for distance vectors among neighbouring nodes can be based on a predefined interval. The exchanging can also be triggered by the change of link cost or the failure of the link/node. In this paper, we consider cases when Ni receives a distance vector from a neighbouring node N_j. Each element of a distance vector received from a neighbouring node N_j includes a destination node t and a delivery cost WN_j; t from the node N_j to the destination node t.

4. RESULT AND ANALYSIS

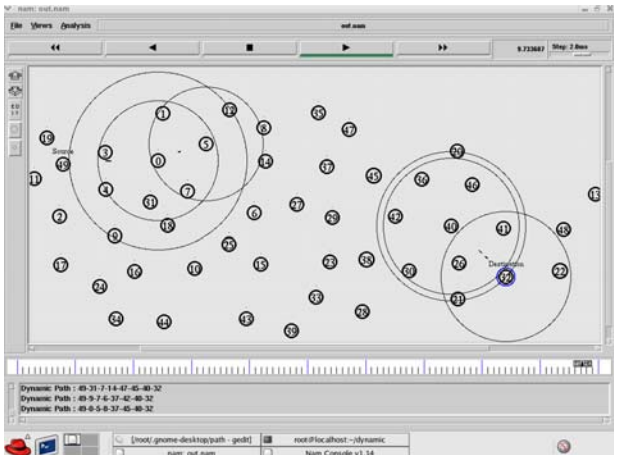
To spot all the structural, syntactical and integration errors in the code, a series of test cases are prepared and the application was tested rigorously using these cases. The system passed most of these, and in case of any discrepancy from the expected behaviour, that portion of the module was immediately modified to make it error free. The test cases used to evaluate the system are given below:



- **Test Case 1:** When a link/node failure is occurred.

Expected Result : When a link/node failure is occurred, the data packets are transmitted by using the backup route.

Observed Result : Same as expected result.



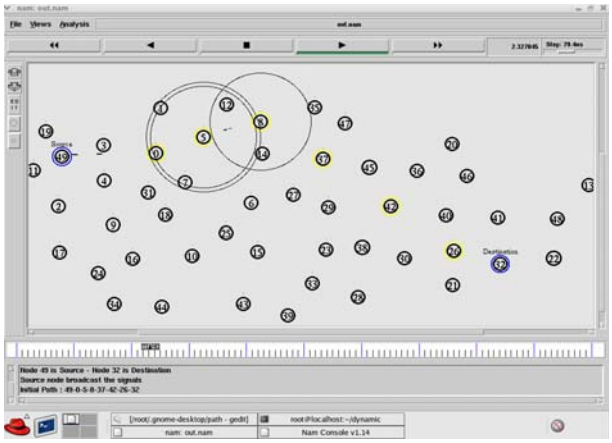
Test case 1

Test Case 2 : When a link/node failure is recovered.

Expected Result : When a link/node failure is recovered, the data packets are transmitted by using the original route.

Observed Result : Same as expected result.

ISSN 2348 – 7968



Test case 2

The simulation results for Hybrid broadcast Routing with Security Consideration under different mobility patterns and traffic scenarios show that the proposed protocol is as efficient as ZRP in discovering and maintaining routes. However, the impact of the overhead caused is almost insignificant and negligible as compared to the proposed degree of security, which provides compared to its other counterparts.

5. CONCLUSION AND ENHANCEMENTS

This paper has proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and DSDV, over existing infrastructures. An analytic study was developed for the proposed algorithm and was verified against the experimental results. A series of simulation experiments were conducted to show the capability of the proposed algorithm, for which we have very encouraging results. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Our security enhanced dynamic routing could be used with cryptography based system designs to further improve the security of data transmission over networks.

Satellite network capacity, adaptability, and responsiveness are enhanced with onboard capabilities for packet switching, bandwidth allocation, and spotbeams which facilitate uplink and downlink spectral reuse. A recent over-the-air (OTA) test of the SPACEWAY system, a Ka-band regenerative satellite mesh network supporting IP packet services, provides definitive demonstration of key capabilities in the areas of quality-of-service, routing for unicast and multicast (both best-effort and guaranteed service) traffic, dynamic bandwidth resource allocation, security, and configurable satellite uplink and downlink components. Leveraging SPACEWAY system technologies and operational capabilities serves as a pragmatic step toward the development of future multi-satellite networks with more advanced features including onboard packet routing, multi-mode radio transmission, and inter-satellite links, which are now being considered for transformational satellite networks.

REFERENCES

1. Dynamic routing with security Considerations IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL.20, NO.1, JANUARY2009 Chin fu kuo , Member, IEEE , Ai-Chun Pang , Member , IEEE .
2. I.Gojmerac, T.Ziegler, F. Ricciato and P. Reichl "Adaptive Multipath Routing for Dynamic Traffic Engineering" Proc. IEEEGlobal Tele Communications Conference.
3. Secure Sockets Layer (SSL), http://www.openssl.org/, 2008.
4. C. Hopps, Analysis of an Equal-Cost Multi- Path Algorithm, Request for comments (RFC 2992), Nov. 2000.
5.V. Pauli, J. Naranjo, E. Seidel, Heterogenous LTE Networks and Intercell Interference Coordination; 2010
6. 3GPP, Requirements for further Advancements for E-UTRAN (LTEAdvanced), 2011
7. C. E. Shannon, A Mathematical Theory of Communication, 1948
8. I. E. Telatar, Capacity of Multi-Antenna Gaussian Channels, 1999
9. ZTE, Discussion of CRS Interference and CSI Measurement in Macro-PicoDeployment, 2010
10.] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha,"Securing Electronic Commerce: Reducing the SSL Overhead,"IEEE Network, 2000.
11. S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing Security via Stochastic Routing," Proc. 11th Int'l Conf.Computer Comm. and Networks (ICCCN), 2002.
12. D. Collins, Carrier Grade Voice over IP. McGraw-Hill, 2003.
13. T.H. Cormen, C.E. Leiserson, and R.L. Rivest, Introduction to Algorithms. MIT Press, 1990.
14. P. Erdo¨s and A. Re´nyi, "On Random Graphs," Publicationes Math.Debrecen, vol. 6, 1959.
15. M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationships of the Internet Topology," Proc. ACM SIGCOMM'99, pp. 251-262, 1999.
16. FreeS/WAN, http://www.freeswan.org, 2008.
17. I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.
18. C. Hopps, Analysis of an Equal-Cost Multi-Path Algorithm, Request for comments (RFC 2992), Nov.2000.
19. C. Kaufman, R. Perlman, and M. Speciner, Network Security PRIVATE Communication in a PUBLIC World, second ed. Prentice all PTR, 2002.
20. J. Katz, M.Yung, " Scalable Protocols for Authenticated Key Exchange", Advances in Cryptology - EUROCRYPT'03, Springer-Verlag, LNCS Vol 2729, pp. 110-125, Santa Barbara, USA [8] 21. W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," Proc. IEEE Military Comm. Conf. (MilCom), 2001.
22. J. Moy, Open Shortest Path First (OSPF) Version 2, Request for comments (RFC 1247), July 1991.
23. C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM '94, pp. 234-244, 1994.

Mr. Jangapally Thirupathi, post graduated in C.S.E M.Tech from JNTUH and graduated in C.S.E B.Tech from JNTUH, AP, INDIA, having 8+ years of teaching experience, presently working as an Associate Professor in Department of computer science engineering, College of Engineering and Technology in Samara University ,Samara, ETHIOPIA, Research interests include: cloud computing data mining and information security

Mr. **K.Ramakrishna**, post graduated in (CSE-SE) M.Tech from JNTUH and graduated in (IT) B.Tech from Kakatiya university, Warangal ,AP, INDIA, he has 5+ years of teaching experience, He is working presently as an Asst.Professor in Department of computer science engineering ,College of Engineering and Technology in Samara University ,Samara, ETHIOPIA, his research interests include mobile ad-hoc networks ,information security and communication