ISSN:0975-9646

Double Layer Security in the Swarm Intelligence P2P Network

K.Ramalakshmi[1], P.K.Sasikumar[2]

[1] *P.G Scholar Computer Science Eng,* [2] *Assistant Professor,*

Dept. of CSE, Tamilnadu College of Engineering, Coimbatore, India.

Abstract **-- Peer-to-peer network has a distributed network architecture with participants can share a portion of their resources such as processing power, network bandwidth directly to network participants and disk storage without the need for central coordination instances. Peer-to-peer content distribution makes the authentication difficult because of the lack of a central authority. Without any authentication adversary nodes can spoof the identity and spoil the integrity by falsifying the messages in the overlay. This enables malicious nodes to launch man-in-the-middle or denial-of-service attacks and many security related attacks. P2P systems require a sufficient amount of trust from the nodes which are all participates in the network. It aims to provide security to decentralized p2p network by the implementation of key server and Intrusion Detection System (IDS) with advanced P2PHBA algorithm can be used for the prediction of optimized path in the network by the scout bee implementation to the efficient file sharing.**

Keywords – Distributed network, double layer security, key server, intrusion detection and prevention system, monitoring, threshold value.

I. INTRODUCTION

Peer-to-peer network each node participates may act as providers and consumers of network services simultaneously which contrasts with the traditional client-server service model computation where the clients only consume the server's resources. In a P2P network the pattern is symmetric because with P2P an end user uploads while downloading files. Every node is designed to(but may not by user choice) provide some service that helps other nodes in the network to get service with two phases discovery phase delivery phase. P2P systems essentially require a broadcast mechanism use a series of unicast or broadcast packets. Each node potentially has the same responsibility. The P2P applications have been enhanced and have growth in recent years because of their low cost, high availability of large numbers of computing and storage resources and network connectivity. Main Design Goals of the P2P system are ability to operate in a dynamic environment, performance, scalability, reliability, anonymity and accountability. Largely used for sharing of content files such as data, audio, video or anything in a digital format with many p2p protocols such as eDonkey, Ares or Bittorrent. Can also be used for business solutions where the companies no need to have resources available to implement a server solution because peers are both suppliers and consumers. In other ad-hoc networks the addition and the removal of nodes may not have significant impact on the network. But this distributed architecture allows peer-to-peer systems to take any topology at any time and to provide enhanced scalability and service robustness. P2P applications like Bittorrent create the overlay networks over the existing physical underlying network in order to perform the functions which is not available in the existing network i.e., indexing and peer collection functions.

Has structured P2P with connections in the overlay are fixed and DHT indexing and unstructured with no algorithm for organization or optimization where connections in the overlay are created arbitrarily. Other types are centralized where central server is used for indexing functions with bittorrent, hybrid with two groups of clients: client and overlay, pure where equipotent peers all peers have equal amount of power. Advantages include the more nodes that are part of the system demand increases and total capacity of the system also increases, there is no single point of failure due to robustness of the system all clients provide to the system.

A. Swarm Intelligence

Swarm-based algorithms have been followed and admired by the behavior of some social living beings such as termites, fishes, birds and ants. Self-organization and decentralized control are most important and remarkable features of swarm-based systems and in nature it leads to an emergent behavior. Emergent behavior is implemented through the local interactions among such system components and it will not possible to be done by any of the components of the system which is acting alone swarm intelligence algorithms were devised for continuous optimization problems. Two important principles of swarm intelligence are self-organization which is based on activity amplification by the positive feedback and activity balancing by the negative feedback and amplification of random fluctuations multiple interactions and second one is stimulation by work which is based on work as a behavioral response to the environmental state where an environment may serve as a work state memory that does not depend on the specific agents.

B. Differ from Other Search Methods

Swarm Intelligence based optimization algorithms aims to provide the optimal solution with difference from direct search algorithms such as random walk and hill climbing is that instead of a single solution SIOAs use a population of solutions for the every iteration. As a population of

solutions is processed in the iteration the population of solutions will be the outcome of each of the iteration. SIOA population can be used to converge to the optimum solution if an optimization problem has a single optimum. However if an optimization problem has multiple optimal solutions an SIOA can be used to capture them in its final population. SIOAs include the Ant Colony Optimization (ACO) algorithm, the Genetic Algorithm (GA) and the Particle Swarm Optimization (PSO) algorithm. Common to all population-based search methods SIOA generates variations of the solution being sought. Some search methods like greedy criterion can be used for the decision on which generated solution to retain. Such a criterion can accept the new solution if it increases the value of the optimized result. Swarm intelligence has also been applied for data mining.

Swarm based P2P model uses Alliance theory for peering where high contributing nodes (Power Nodes) have high ranking based on their share ratios and nodes may be served by the direct server and in small world networks every node can also be connected to every other node in the swarm by the small number of path length. Alliance members have common trust and treaty as a node receives new content it forwards among its alliance members first alliance members are mutually trusted and all members of an alliance have an active connection with other members and also applying security policies in alliance is much easier.

C. Honey Bee Algorithm

Artificial bee colony algorithm (ABC) is a meta-heuristic algorithm In the ABC model the colony consists of three groups of bees called onlookers, employed bees and scouts. Here it can be assumed that for each food source there is only one artificial employed bee i.e., the number of both employed bees in the colony and the food sources around the hive are equal. After reaching their food source employed bees come back to the hive and dance on this area. The employed bees which are all having the abandoned food source become a scout and start to search for finding a new food source. After watching the dances of employed bees, depending on dances the onlookers choose food sources. The main steps of the algorithm are given as

1. Initial food sources are produced for all employed bees.
2. REPEAT
3. Each employed bee can reach the food source in her memory and identifies the neighbor source after that can calculates its nectar amount and dances in the hive
4. After watching the dance done by the employed bees, each onlooker chooses their sources based on the dances, and then goes to that source. Nectar amount can be evaluated after choosing a neighbor around the onlooker bees. .
5. Abandoned food sources can be replaced with the new food sources discovered by scouts.
6. The best food source found so far is registered.
7. UNTIL (requirements are met)

In ABC a population based algorithm the possible solution to the optimization problem can be represented by the position of a food source and based on the quality (fitness) of the associated solution the nectar amount of a food source be calculated. The number of employed bees in the colony and the number of solutions are equal. At first step a randomly distributed population get (food source positions) initially generated. After initialization the cycles of the search processes of the employed bees, onlooker bees and the scout bees are repeated respectively. To discover a new food source position an employed bee makes the modification on the source position in her memory. The bee memorizes the position of new source and forgets the old source position when the nectar amount of the new source is higher than that of the previous source .Otherwise employee bee keeps the position of the one source in her memory. After the completion of search process all employed bees can share the position information of the sources with the onlookers on the dance area. Depending on the nectar amounts of the sources which are all shared from all employed bees each onlooker bees evaluates the nectar information for choosing the best food source . Same as the employed bees, onlooker bees also makes the modifications on the source positions in her memory and checks for new nectar amount. The bee memorizes the position of new source and forgets the old source position when the nectar amount of the new source is higher than that of the previous source. After the determination of abandoned sources new sources can be produced to be replaced with the abandoned ones by the artificial scout bees.

D. Security Challenges

Differentiation from client-server systems like central authority makes many security challenges to the P2P systems. Peer-to-peer content distribution makes the authentication difficult because of the lack of a central authority. Without any authentication adversary nodes can spoof the identity and spoil the integrity by falsifying the messages in the overlay. This enables malicious nodes to launch man-in-the-middle or denial-of-service attacks and many security related attacks. Without a trusted agency which certifies identities adversary nodes can control a large fraction of an overlay network. Three most important requirements for secured overlay network are secured node-ID assignment, secured routing table maintenance and secured message forwarding . Threats specific to P2P-SIP are bootstrapping communications in the presence of malicious first-contact nodes, subversion of the identity-mapping scheme attacks on the overlay network routine scheme, traffic analysis and privacy violation by intermediate nodes, identity enforcement (Sybil attacks) and free riding by nodes that refuse to route calls but participate in the protocol to obtain service for themselves (selfish behavior).

The modern P2P systems need to deal with selfish (a.k.a “leechers” or “free-riders”) or malicious users, P2P worms , Byzantine faults and Sybil attacks, Eclipse attacks, flash crowds, etc.

In this paper initial distribution of scattered nodes with key server and IDS implementation will achieve better availability, authority and authentication of information by identifying and preventing the malicious nodes.

II. RELATED WORKS

In this paper the author has concentrated on trusted computing technology in which a pseudonymous authentication scheme for peers to reduce pseudospoofing and provides anonymity for users and eases discovery of resources and routing of resource queries in P2P network. Trusted Computing Group (TCG) protocols for Direct Anonymous Attestation (DAA) specifications with Trusted Platform Module (TPM) can be used to provide robust access control, data integrity and confidential services. Sign and verify algorithm will be used by the peers for the authentication in the network[17].

In this paper the author has proposed a unique poisoning-resistant security framework can effectively and efficiently defend against content poisoning happened through man-in-the-middle (MITM), Sybil and DoS attacks by the implementation of trusted sources to verify the integrity of the requested content would be the content providers. A content provider broadcasted the information of their own shared contents to all nodes also act as a content provider/maintainers can organize itself in a security overlay to achieve the data's availability and scalability. Based on these content requestor can achieve the integrity of the requested content from the associated content provider/maintainer. Here scalable probabilistic verification scheme to reduce the verification overhead and to enhance the system performance [15].

In this paper the author has proposed the origin server (OS) and Trust Index Table (TIT) can be used with trust value calculation based on success of data delivery ratio and search time for trusted nodes to increase the success ratio with reduced delay and drop. Query sending rate is from 250Kb to 1Mb increases when trust evaluation is applied. Delay is decreases at trust evaluation and drop is constant in the trust based case [6].

In this paper the author has proposed the Identity-based encryption to be useful in pre-distribution of authenticated keys is inconvenient and to eliminates the need for a public key distribution infrastructure. Also the implementation of private key generator (PKG) achieves the distribution of the private keys and to decrypt or sign the messages. This has RSA algorithm like asymmetric key algorithms for safer data replication, authenticity, integrity, confidentiality, reduces overheads, query efficiency, high replica hit rate and to prevent sybil attacks [18].

In this paper the author has proposed the peer authorization protocol (PAP) for the identification of malicious nodes in the network by differentiating the legal nodes from illegal nodes. Private key generator (PKG) will achieve better system performance, minimum delivery cost, maximum content availability less overhead. Identity-based signatures (IBS) can be used for the authorization and verification. Implementation of gossip trust system time stamped tokens to identify the pirated copies through secure file indexes with swarm size of 2,000 peers can be handled by 10 PC-based distribution agents. NAT device and digital rights management (DRM) techniques for higher content availability, system performance, less overhead and minimum delivery cost. This paper has achieves 99.9 percent of illegal prevention rate in Gnutella, KaZaA, and freenet and also 85-98 percent prevention rate on eMule, eDonkey, Morpheus [20].

In this paper the author has proposed the symmetric encryption and public key encryption for reliable and secure content distribution. Search for Extraterrestrial Intelligence (SETI) can use the accountability mechanism to replicate all computation for the quality control. Using the gossip model initial node discovery and subsequent network maintenance are done. Network Address Translator sends the packet to final destination through internet in a secured through tunnel with Groove's decentralization improves the robustness. Signature verification keys and digital signature implementations can achieve fault tolerant, survivable, highly scalable, flexible, expected latency, robustness, authenticated, confidential nodes with integrity of messages, high robust anonymity and document durability in the network [1].

III. QOS AWARE CONTENT DISTRIBUTION

Topology formation is implemented in the network will set the initial design of the proposed model and the initial broadcasting will occur and the topology discovery process will be occured.

A. Dynamic Source Routing Protocol

DSR is a reactive routing protocol with no periodic table-update messages like table-driven routing protocols to manage a MANET. It is specifically designed for use in multi-hop wireless ad hoc networks where the protocol allows the network to be completely self-configuring i.e., self-organizing where there is no need for an existing network infrastructure or administration. Only at the time routing i.e, a path is required by a node (On-Demand-Routing) the process to find a path is get executed to restrict the excessive use of bandwidth. In DSR the source node (sender, initiator) first determines the communication path to reach the destination node (Source-Routing) and then deposits the intermediate node addresses in the packets. Compared with other reactive routing protocols like SSA or ABR DSR will be beacon less that is there is a no need of hello-messages by the nodes to notify their neighbors about their presence. DSR was developed for MANETs with a moderate speed at small diameter of 5 to 10 hops. DSR uses the Link-State-Algorithms that is each node can be able to save the best way to a destination. Whatever may be changes were made in the network topology will be broadcasted to the whole network by flooding. DSR contains 2 phases Route Discovery (find a path), Route Maintenance (maintain a path).

Route Discovery

If node 1 has in his Route Cache a route to the destination 5 then this route is immediately used. If it is not then the Route Discovery protocol is started.

Route Maintenance

In DSR every node has the responsibility to confirm that the next hop in the source route receives the packet and also to confirm that each packet gets forwarded only once by a node (hop-by-hop routing) except for the lost packets. If a particular packet can't be received by a node then the

lost packet can be retransmitted to some extent until a confirmation is received from the next hop. A RouteError message is sent to the initiator at the retransmission failure then the particular source route will be removed from the route cache. So the initiator can check his route cache for efficient some other route to reach the target. If there is no route in the cache then a RouteRequest packet is broadcasted to identify new routes.

Advantages of reactive routing protocols include that there will be no need of flooding the network periodically to update the routing tables like table-driven routing protocols do. Control overhead can be reduced by the efficient utilization of Route Cache information by the intermediate nodes. If there is no route in the cache then only initiator tries to find a route (path). Without the need of hello messages peers can advertise themselves will save the current and bandwidth usage (beacon-less). For future implementations AODV routing also will be used.

B. AODV ROUTING

The combination of DSDV and DSR produce ad hoc on demand distance vector routing (AODV). Routing table is maintained by each node in AODV and each routing table entry will contain the active neighbor list and those neighbor nodes in this list will be informed the destination address, next-hop address toward that destination, number of hops to destination, sequence number, lifetime when the link in the entry is broken.

Routing in AODV consists of two phases called Route Discovery and Route Maintenance. Whenever a source node wants to communicate with a destination it looks up in the routing table. If the destination node is found in the routing table then the source node transmits the data in the same way as in DSDV. If the source node can't get the path for communication then it starts Route Discovery mechanism and broadcast the Route Request packet to its neighbor nodes. The source node can rebroadcast this request to their neighbor nodes until it finds the possible way to the destination. Whenever the node between the source and destination receives a RREQ then the node will update the route to previous node and checks for the following two conditions to satisfy (i) whether there can be an accessible entry with the same destination address as in the RREQ (ii) whether has a greater or equal sequence number as in the RREQ. If it is not present then it will be rebroadcasting the RREQ message. If it finds any node like that then it generates a RREP message to the source node. Using the routed back RREP message the nodes in the reverse path updates their routing table with the new added next hop information. If a node receives a RREQ then it checks the sequence number and discards the RREQ to prevent the loop. If the source node receives more than one RREP message then the reply message with greater sequence number will be chosen. If two RREPs with the same sequence number then reply message with less number of hops to reach destination will be chosen. When a route is found it will be maintained by the route maintenance mechanism where each node send hello packet to the neighbors periodically to prove its presence and availability because when there is no hello packet get received from a node with in a particular time the connection to that node will be considered to be broken i.e., the node which didn't receive any hello message will invalidate all of its related routes as failed node and may inform that to other neighbor by Route Error packet. If the source still want to transmit data to the destination will get a new path by the restart of Route Discovery. AODV includes the advantages of low processing, quick adapt to net work topology change, decreasing the overhead control messages, more scalable up to 10000 mobile nodes.

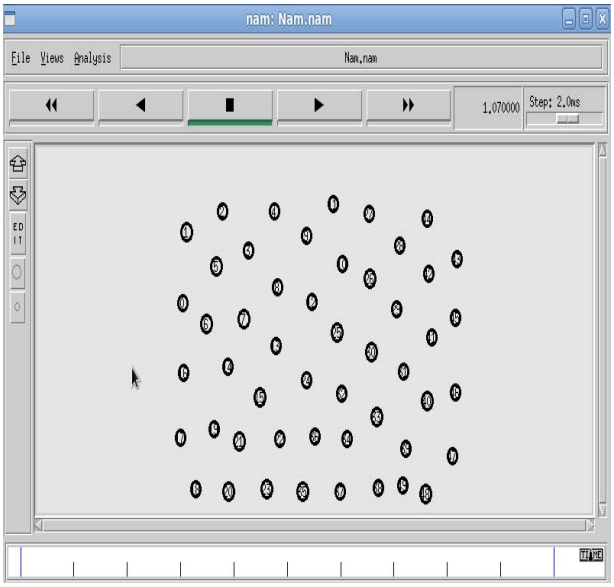

Fig 1: Topology of P2P overlay network

C. INTRUSION DETECTION AND REVENTION SYSTEM

An intrusion detection system (IDS) is a security providing device or a software application that can be able to monitor the network or system activities for malicious activities and policy violations for producing the reports to a management station. Intrusion prevention systems (IPS) or intrusion detection and prevention systems (IDPS) are a security providing network appliances that can be able to monitor the network and/or system activities for malicious activity i.e., mainly responsible for the identification of possible malicious incidents, log those information, reporting attempt, documenting existing threats, identify the problems corresponds to security policies and deterring individuals from violating security policies. IDPSes can respond to a detected threat by the attempts to prevent it from succeeding which may involve the IDPS stopping the attack itself, changing the security environment such as reconfiguring a firewall or changing the attack's content. The major differences between IDS and IPS are different from intrusion detection systems, intrusion prevention systems can be placed in-line and are able to prevent/block the intrusions that are identified/detected. IPS can take such actions as sending an alarm, resetting the connection, dropping the malicious packets and/or blocking the traffic from the offending IP address. Cyclic Redundancy Check (CRC) errors unfragment packet streams can be corrected and prevented by an IPS also is concentrate on TCP sequencing issues and clean up unwanted transport and

network layer options. In a passive system the intrusion detection system (IDS) sensor detects the potential security breach, logs the information and signals an alert to operator. In a reactive or an intrusion prevention system (IPS) the IPS auto-responds to the malicious activity by terminating or resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source. The term IDPS is commonly used where this can happen automatically or at the command of an operator systems that both "detect (alert)" and "prevent".

D. Comparison with Firewall

Eventhough IDS and firewall are relate to network security an intrusion detection system (IDS) can be differentiated from a firewall in that the firewall monitors the network to stop the intrusions from happening and it also limits the access taken between the networks to avoid intrusion and do not signal an attack from within the network. But opposite to firewall after the interception of an intrusion IDS signals an alarm and also watches for an attack happened or originated from inside a system. This can be achieved by monitoring or examining the network communication activities, identifying the signatures called heuristics and patterns of common computer attacks and taking action to those illegal activities by giving the alert to the operators. An intrusion prevention system is a system in which it terminates the connection to prevent the unwanted activities and is another form of an application layer firewall.

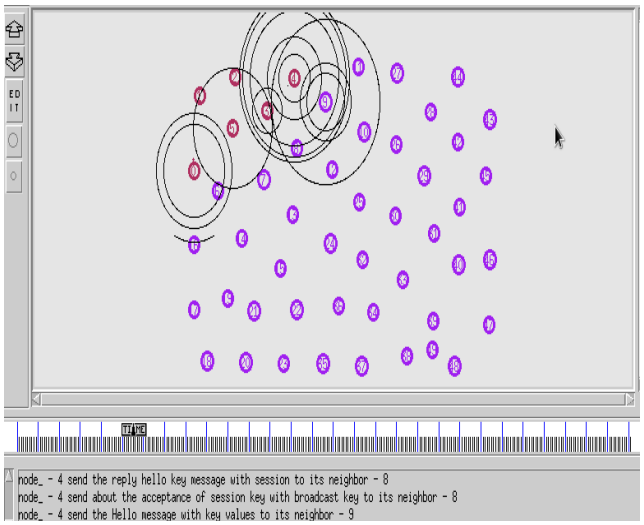

Fig 2: Key Server to distribute public keys to nodes

Key Server is distributing the public keys to all nodes in the network. Keys will be act according to private key to individual nodes when participating in data sharing between them. Some nodes in the network will act as IDS to monitor the nodes around the node. It can also act as a cluster to achieve second wall of defence against intruder in the operation. This cluster form of monitoring will also decrease the overhead which may be happened while cluster head has maintaining the routes. For the dynamic routing purpose nodes outside the network coverage need to get authenticated by Intrusion Detection System (IDS).

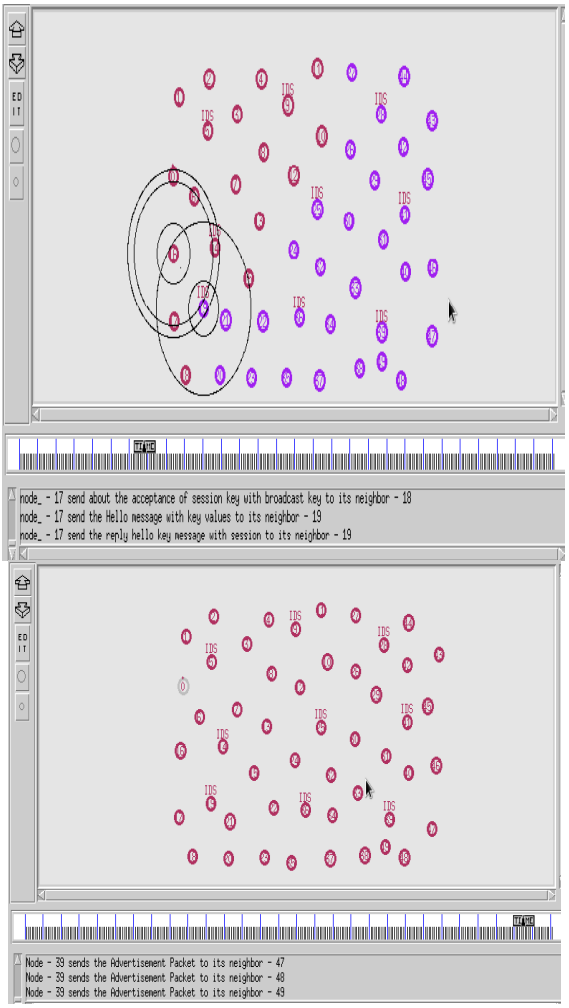

Fig 3: Implementation of IDS and key server to monitor the nodes

IV. CONCLUSION AND FUTURE WORK

Implementation of key server is to provide public key to all nodes in the network at the configuration period for first layer security. At the time of routing Intrusion Detection System (IDS) is initiated for monitoring the nodes which also act as a cluster to achieve second wall of defence against intruder in the operation. This cluster form of monitoring will also decrease the overhead which may be happened while cluster head has maintaining the routes. IDS will identify the nodes as trusted and un trusted based on some threshold values and also inform about untrusted to all nodes in the network to transfer data in a secured manner. For the dynamic routing purpose nodes outside the network coverage need to get authenticated by IDS. Nodes which are all having the value above threshold value will be treated as trusted nodes will be taken into routing between the source and destination. Untrusted nodes which are all identified by the IDS will not be taken into account and the corresponding information is forwarded to all the nodes in the internet. Also IDS will consume less energy than other security providing mechanisms without affecting the performance. Monitoring allows somebody to detect, analyze and recover from detected faults, providing additional defence against catastrophic failures. By using these methodologies QoS is achieved with better security.

REFERENCES

[1] Allan Friedman, L Jean, *Peer-to-Peer Security* Telecommunications Policy Research Conference, Washington DC, September, 2003.

[2] Anandaraj M, Dr Ganeshkumar P, Vijayakumar K P, *An Efficient QOS Based Multimedia Content Distribution Mechanism in P2P Network* ISSN: 2277 128X ,International Journal of Advanced Research in Computer Science and Software Engineering, May,2013.

[3] Anna Saro Vijendran, S Thavamani, *An Efficient Algorithm For Clustering Nodes Classifying And Replication Of Content On Demand Basis For Content Distribution In P2P Overlay Networks* International Journal of Computer & Communication Technology ISSN (Print): 0975 – 7449, 2013.

[4] Anusuya.R, Dr Kavitha V, Mrs Golden Julie E, *Enhancing and Analyzing Search performance in Unstructured Peer to Peer Networks Using Enhanced Guided Search Protocol (EGSP)* , ISSN 2151-9617 Journal of Computing, Volume 2, Issue 6, June, 2010.

[5] Ayyasamy S, Sivanandam S N,*A Cluster Based Replication Architecture for Load Balancing in Peer-to-Peer Content Distribution*, International Journal of Computer Networks & Communications (IJCNC) September, 2010.

[6] Ayyasamy S, Sivanandam S N, *Trust Based Content Distribution for Peer-To-Peer Overlay Networks*, International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April, 2010.

[7] Christian Rohner, *Security Bootstrapping for Networked Devices*, European Workshop on Security in Ad-hoc and Sensor Networks - ESAS , pp. 165-178,2006.

[8] Esther Palomar Juan M. Estevez-Tapiador Julio C. Hernandez-Castro Arturo Ribagorda, *A Protocol for Secure Content Distribution in Pure P2P Networks*, DEXA Workshops 2006: 712-716. Proceeding 6 Proceedings of the 17th International Conference on Database and Expert Systems Applications ISBN:0-7695-2641-1, 2006.

[9] Fang Zhao, Ton Kalker, Muriel Medard and Keesook J. Han, *Signatures for Content Distribution with Network Coding*, In Proc. of International Symposium on Information Theory (ISIT), 2007.

[10] Heba A, Kurida, Thanaa S, Alnusairib, Hajar S, Almujaheda Heba A Kurid, *OBAME: Optimized Bio-inspired Algorithm to Maximize Search Efficiency in P2P Databases*, The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN), 2013.

[11] Heng He, Ruixuan Li, Guoqiang Gao, Zhiyong Xu, Weijun Xiao, *An Integrated System Solution for Secure P2P Content Distribution Based on Network Coding* Proceedings of NAS '11 Proceedings of the 2011 IEEE Sixth International Conference on Networking, Architecture, and Storage, 28-30 July 2011, 191-196, ISBN: 978-0-7695-4509-7, 2011.

[12] Jing Zhao, Ping Zhang and Guohong Cao, *On Cooperative Caching in Wireless P2P Networks*, National Science Foundation (NSF) under grant CNS-0721479, Aug 24, 2013.

[13] Laurent Eschenauer, John S. Baras, Virgil Gligor, *Distributed Trust Establishment in MANET's: Swarm Intelligence*, 2003.

[14] Majd ghareeb, Soufiane rouibia, Benoît parrein, Mohamad raad, Cedric tharea,*P2PWeb: a Client/Server and P2P Hybrid Architecture for Content Delivery over Internet*, In Third International Conference on Communications and Information ICCIT, 18 July, 2013.

[15] Ruichuan Chen, Eng Keong Lua, Jon Crowcroft, Wenjia Guo, Liyong Tang, Zhong Chen, *Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks* pp. 22-29, 8th International Conference in p2p computing, IEEE, 2008.

[16] Sabu M. Thampi, Chandra Sekaran K, *Protocols for Bio-Inspired Resource Discovery and Erasure Coded Replication in P2P Networks* INFOCOMP Journal of Computer Science, ISSN 1807-4545, June, 2010.

[17] Shane Balfe, Amit D. Lakhani and Kenneth G. Paterson, *Trusted Computing: Providing Security for Peer-to-Peer Networks*, Fifth IEEE International Conference on Peer-to-Peer Computing (P2P 2005), 31 August - 2 September 2005, Konstanz, Germany. IEEE Computer Society 2005 ISBN 0-7695-2376-5,Stamp Collectors Against Dodgy Sellers (SCADS) institute, 117-124, 2005.

[18] Vijaya Bharath K., Praveen Kumar B.,. Rajagopalan S.P, *An Identity-Based Security for Nodes in EAD File Replication in P2P Systems*, ISSN: 2278-5183 International Journal of Computers and Distributed Systems www.ijcdsonline.com Vol. No.1, Issue 3, October 2012 88, 2012.

[19] Vladimir Gorodetsky, Oleg Karsaev, Vladimir Samoylov, Sergey Serebryakov, *Multi-agent Peer-to-Peer Intrusion Detection*,260-271, Fourth International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2007 St. Petersburg, Russia, September 13–15, 2007 Proceedings, ISBN 978-3-540-73985-2, 2007.

[20] Xiaosong Lou and Kai Hwang, *Collusive Piracy Prevention in P2P Content Delivery Networks*, Published by the IEEE Computer Society, IEEE transactions on computers, VOL. 58, NO. 7, july 2009,0018-9340/09/$25.00 _ 2009 IEEE 2009.

[21] Yuting Liu, Xiaofeng Qiu, Yang Ji, Chunhong Zhang *A Novel Security Mechanism to Defend Cross-layer Security Threats in P2P Network*,978-1-4244-7255-0/11/$26.00 ©2011 IEEE, 2011.

[22] zakiya M. tamimi, *Automated Peer-to-Peer Security-Update Propagation Network*, Proceeding ICCOMP'07 Proceedings of the 11th WSEAS International Conference on Computers, 557-564, ISBN: 978-960-8457-95-9,2007.