INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Secured BGP Routing Protocol For Network Services

J. Viba Mary
Assistant Professor, St.Paul's College Of Arts & Science

Abstract:
Computer Network have pervaded each and every day in our life and also prevent in all aspects. Now everyone knows that network services are provided by service gateways, where it only focused on minimizing the length of the routes have an overall network performance. As more and more people use computer networks, traffic increases so it puts a heavy toll on the infrastructure delivering the data from source to destination where it leads to delayed data, data variation, throughput of messages and packet loss. For this problem Reuven Cohen [1] showed that, the placement and selection of network services can be used as an effective tool for traffic engineering in that literature. In that the problem was divided into two sub problems: 1) finding the best location for service gateway, 2) selecting the best service gateway for each flow which focuses on placing the service gateways in a way that minimizes the average length of the traversed routes. Approximation algorithm and heuristics were used for the selection problem. But in this paper, the main contribution is showing that the BGP protocol can address the task of determining the path by using SPF algorithm to find the shortest path route to reduce the congestion of traffic in the network services. And there are many malicious behaviour actions that can be carried out to attack a Wireless Sensor Network while routing. So to overcome this problem a special securing topology maintenance protocol called Meta protocol (Meta-TMP) are also used in this article in order to provide security and high performance for wireless sensor networks.

1.Introduction

The development of computer Networks has given rise to the Internet, where millions and millions of data bytes are transferred each and every second across the world. The “Internet” was the short form of the international network. It was also known by different names such as information super highway. It plays a significant role in the day- to day affairs of the society, ”Internet” is defined as a date of communication system that interconnects computer’s systems at different sites.

As the internet becomes more prevalent and diverse, there was a growing demand for services that facilitate and performance, enhance interoperability, and security of communication between two parties, i.e. the source and destination. Examples of such services are voice and video conversion, protocol translation, QOS control, authentication, caching, encryption, compression, intrusion and detection. These services require the service gateway such as firewalls, VOIP gateways, NAT routers, VPN gateways and broadband assess servers.

The quality of service (QOS) was generally measured in the time required by the packets take to reach the destination from the source. It also measures the data variation, data loss, throughput of messages, delay variation and delay that takes place between the source and destination during the transaction, depending on network traffic and capacity. So network generally has ingress traffic and egress traffic. Normally the serviced traffic traverses the shortest path from the source to the service gateway and then to the destination.

Security was very critical for wireless sensor network applications like military surveillance, emergency response and medical monitoring. There are many security mechanisms developed for the internet but it cannot be applied directly to Wireless Sensor Networks due to their limited resource in computation, memory, communication bandwidth and energy. Nowadays, it is impossible to include strong security mechanisms for each of the services at a node such as routing, localization, time synchronization, power management, sensing and medium access control. Moreover, even if a secure routing protocol is implemented to protect the internet, it may suffer from low efficiency and will not perform against attacks from other services.

Topology maintenance protocols such as SPAN, ASCENT, PEAS and CPP were critical to the operation of wireless sensor networks. These protocols only aims to increase the lifetime of the sensor network by maintaining a subset of nodes in an active or awake state. There should be enough active nodes of activity on the network and obtain sensing coverage in the area where the sensor network was deployed. The Topology maintenance protocol attacks can be carried out either by external to the network i.e., outsider attacks or by internal to the network i.e., insider attacks.

This paper describes the operation of BGP protocol to determine the task of routing path between two or more inter-autonomous systems of the network and finding the shortest path routing by using an SPF algorithm and routing calculations. To prevent wireless sensor networks from various types of malicious behaviour and attacks a special kind of Topology maintenance protocols such as the Meta - TMP protocol is implemented for secured network.

The rest of the paper is organized as follows. In section 3, the network overview is presented, In section 4, the details of related work is presented. In section 5, SPF algorithm for shortest path routing is explained, In section 6, the routing calculation is done. In section 7, the operation of BGP protocol and its routing is implemented. In section 8, the types of routing attacks are explained. In section 9, the attacker classification is described. In section 10, the brief overview of Meta-TMP protocol is explained. In section 11, the future enhancement is discussed. And in section 12, the paper is concluded.

2.Overview Of Network

When a web page was assessed, a transport layer virtual connection was established from the user's computer to the web server. This request starts data transfer from the web server to the user's computer in blocks known as packets. Packet is nothing but a short fixed-length block of data which is used for transmission. Each packet have bits for control information such as address routing, security, error control, etc… as well as data. These packets will travel through a number of switches and routers. Router is nothing but it can connects one or more networks together and links it with internet. It is linked to a server when a million of users perform the same task, the packets generated do not travel through the same set of switches and routers. These may be a common set of switches and routers.

When a network request was made from the user, the request processed by a number of different networks and through a number of network service providers. The packets that are generated from the source will travel through the network by a path specified by the network parameters and protocols. The packets from the target travel back to the source in the same path unless and until the network provides a different path for some or other reasons. The path travelled by the packets was obtained by switching through different networks of different network service providers. This is called packet switching. It is also defined as an economical way of sending long data over long distances. The data was send from a sending to a receiving terminal or computer in packets of fixed length (1000 bits or so). Each packet was sent separately and may be interspersed with packet from another location.

When two or more networks are involved in transferring packets, there must some amount co-ordination between them. This co-ordination is known as peering. When a packet switches from one to another network, it enters a network through a specific point. This specific point is known as the gateway. Within two gateway lies the network which carries the packet, hence the optimization takes place in this network only. This network is known as the backbone network.

3.Related Work

The problem of placing network intermediate devices to minimize the distance have been extensively addressed in a vast range of fields. Much work has been done on the placement of devices like caches, mirror server [20] and web proxies [7], etc. These devices usually respond only to the service request themselves, they do not forward any traffic to the user node. However, they can consider as private cases of session – oriented services in which the volume of traffic changes after it passes through the service gateway. So these results are applicable to such services as well.

Likewise, another research also have done in that field for intermediate device placement using stream processing system. The goal of the research was to select appropriate device while dynamically adjusting to the network load, thereby minimizing service latency and improving resiliency.

The above related works were mainly focused on placement and selection of intermediate devices while minimizing bandwidth consumption or minimizing the distance between the device and the end users. For that, the graph – theoretic algorithms which are based on approximation algorithms[2] for the K center and K-median[19] problems were used. There are also other algorithms which was based on the greedy strategy[20]. Some papers suggest that placing the service gateways in a distributed manner, so it results in scalable, efficient and adaptable to dynamically changing new conditions. The drawback of the paper was the clients need to continuously relocate the gateway. Another drawback in algorithm was the current load on every network link cannot be delivered to the nodes in real time.

Although many securing routing protocols have been developed for these networks, but it cannot be directly applicable for some reasons. Some protocols like ARAN, SAODV[17] use public-key cryptography, which have low memory as well as low energy. So it cannot be used frequently for sensor networks. Another protocol called SPINS[16], TinySec[9] provides secure channels. They may be used to establish basic shortest-path routing trees, but are inadequate defenses when nodes are compromised. Antony D. Wood, Le Fang[22] had proved that a protocol named as SIGF (Secure Implicit Geographic Forwarding), a secure routing protocol family for wireless sensor networks provides high performance and security with high efficient. Another protocols like SPAN and ASCENT[23] attempt to maintain network connectivity, but do not guarantee sensing coverage. On the other hand, PEAS and CCP[23] are designed to address both connectivity and the application’s coverage requirements in a configurable fashion.

Finally, in this article a new concept called All pairs shortest– path routing algorithm was proposed. In this paradigm, a traffic flow can be routed through up to N intermediate nodes which traversing the shortest paths between them before reaching its destination. It is effective for load balancing and achieving better utilization of new resources. And also a topology maintenance protocol called Meta-TMP protocol is used to provide authentication mechanism for routing path to be secure with high performance and high efficiency.

4.Border Gateway Protocol

4.1.Background

Routing involves two basic activities: determining the optimal routing path and the transporting the information groups i.e., packets through an internetworking. The determination of the path was very complex whereas the transport of packets through an internet work is relatively straightforward. Nowadays the border gateway protocol (BGP) acts as a protocol which is used to address the task of determining the path .

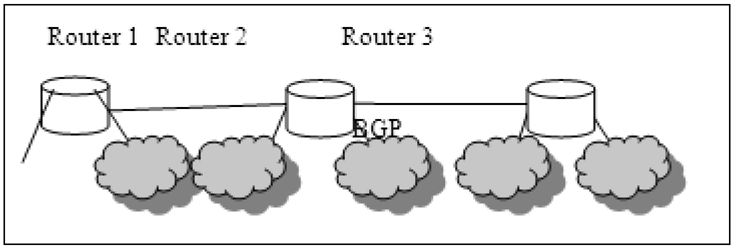


Figure 1: Core Routers Can Use BGP To Route Traffic Between Autonomous Systems

BGP can perform interdomain routing Transmission–Control Protocol / Internet protocol (TCP/IP networks) and routing between multiple autonomous systems or domains and exchanges the routing path and reachability information with BGP systems. BGP is also known as an exterior gateway protocol (EGP).

4.2.BGP Operation

BGP performs three types of routings : i) interautonomous system routing, ii) intra-autonomous system routing and iii) pass-through autonomous system routing.

Inter autonomous system routing occurs in different autonomous systems between two or more BGP routers. Each system has Peer routers which have the access of BGP to maintain a consistent view of the internet work topology. Ex: Internet service.

Intra autonomous system routing is located within the same autonomous system between two are more BGP routers. Here Peer routers are used to maintain a consistent view of the system topology. BGP also used to determine which router will serve as the connection point for the specific external autonomous system. Ex: Internet service (such as university).

Pass-through autonomous system routing that exchange traffic across an autonomous system that does not run BGP that occurs between two are more BGP peer routers.

4.3.BGP Routing

BGP can be able to maintain the routing table which can transmit the routing updates, and bases routing decisions on routing metrics. The base function of a BGP system is to exchange network – reachability information, including information about the list of autonomous system paths, with other BGP systems. The routing table consists of lists of all possible paths to a particular network. The router does not refresh the routing table, however, Instead, the routing information received from peer routers was retained until an incremental update is received.

BGP devices exchange routing information upon initial data exchange and after incremental updates. The routers exchange its entire BGP routing tables , when a router connects to the network. Similarly, when the routing table was changed, then the routers send the portion of their routing table that have changed. BGP routers do not send regularly scheduled routing updates, and BGP routing updates advertise only the optimal path to a network.

BGP uses a single routing metric to determine the best and shortest path to a given network. This metric consists of an arbitrary until number that specifies the degree of preference of a particular link. The BGP metric typically is assigned to each link by the network administrator. The value assigned to a link can be based on any number of criteria, including the number of autonomous systems through which the path passes, stability, speed, delay, or cost.

Many Internet service providers (ISPs) choose intern autonomous system routes by adjusting BGP route attributes in order to optimize their optional IP between neighbouring autonomous systems and to load balance inter- autonomous system traffic. This technique is known as BGP traffic engineering (TE).

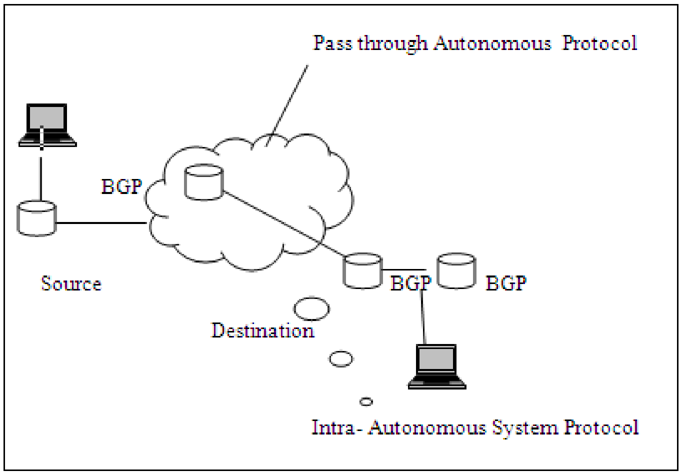

Pass through Autonomous Protocol
BGP
Source
BGP
BGP
Destination
Intra- Autonomous System Protocol

Figure 2: In Pass-Through Autonomous System Routing,
BGP Pairs With Another Intra-Autonomous System-Routing Protocol

5.Methodology

5.1.All Pairs Shortest Path Problem

Let the algorithms is presented for online selection problem. The selection problem can be translated into a special case of a well – known traffic engineering problem called the online unsplittable flow problem. Each and every flow may be routed over an arbitrary route. Likewise, a flow must pass through only in the shortest path and may be routed over a limited set of routes . Thus the results are extended to the general unsplittable flow problem to address our selection problem.

5.1.1.Algorithms

```
Algorithm  AllPaths (cost X, n)
{
   for  g : = 1 to n do
       for  h : = 1 to n do
            X [ g , h ] : = cost [ g , h ] ;
   for  i : = 1 to n do
      for  g : = 1 to n do
         for  h : = 1 to n do
                    X [ g , h ] : = min (X [ g , h ], X[ i , g ] +          X [ i , h ]) ;
}
```

Let G=(V,E) be a directed graph with n vertices. Let cost be a cost adjacency matrix for G such that cost (g,g) = 0,$1\leq g \leq n$. Then cost (g,h) is the length (or) cost of edge. Let cost [1 : n, 1 : n] is the cost adjacency matrix of a graph with n vertices; X[g,h] is a cost of a shortest path from vertex g to h. cost[g , g] = 0.0, for $1 \leq g \leq n$. Let us examine a shortest path g to h in G, $g \neq h$. The path starts from the vertex g and travels through an intermediate vertices and reached at vertex h. Then assume, if K is the intermediate vertices , then g is passed in this shortest path, then the sub path from g to i and k to h must be shortest paths respectively. In this case g to h path is in maximum length so the principle of optimality holds, thus it alerts us to the prospect of using dynamic programming.

The all pairs shortest path problem is used to determine a matrix X such that X (g,h) is the length of a shortest path from g to h. The matrix X can be obtained by solving n single – source problems using the shortest path algorithm. Each application requires $O(n^2)$ time, the matrix X can be obtained only in $O(n^3)$ time. Then an alternate solution $O(n^3)$ was obtained by using the principle of optimality to this problem.

5.1.2.Example

The graph of Figure 1.(a) has the cost matrix of figure 1. (b). The initial X matrix, X^0, plus its value after 3 iterations X^1, X^2, and X^3 are given in figure 1.

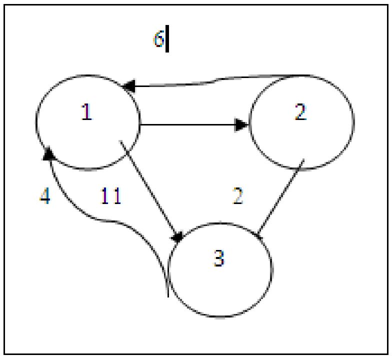
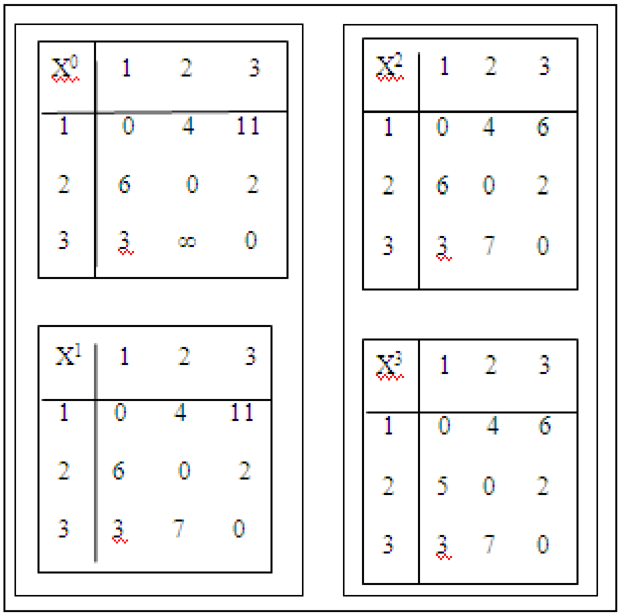


Figure 3(a): Example Digraph



X^0	1	2	3
1	0	4	11
2	6	0	2
3	3	∞	0

X^1	1	2	3
1	0	4	11
2	6	0	2
3	3	7	0

X^2	1	2	3
1	0	4	6
2	6	0	2
3	3	7	0

X^3	1	2	3
1	0	4	6
2	5	0	2
3	3	7	0

Figure 3(b) : Associated Matrices With Directed Graph

5.2.Routing Calculations

The shortest path can be easily determined by using SPF algorithm. Some of the features are:

- It is very simple to implement.
- It is also known as Dijiktra’s algorithm.
- It is one of the popular method for calculating best paths.
- Link-state protocols are also called as SPF–based protocols.
- It is efficiency.

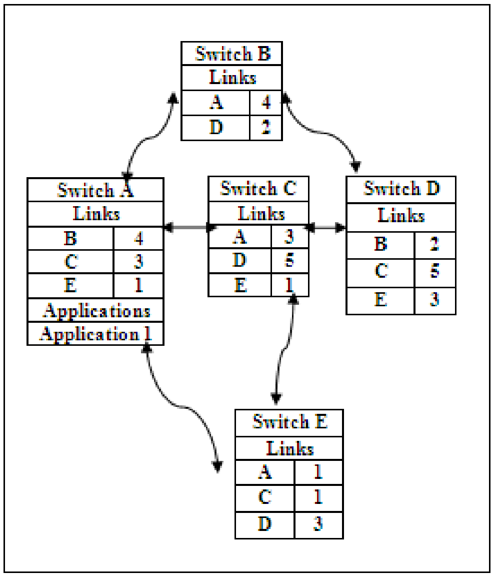


Figure : 4

Here the Dijiktra's algorithm is used for routing calculation. For this, each link should be assigned a non-negative cost. Here the cost of the path is the sum of the cost of the links which is making up the path. By using all other switches in the network it will calculate and produces a set of shortest paths in the network. There are two types of disjoint sets of switches. One switches consist of shortest path have already been found and the other set switches where candidate paths have been found.

Explanation: In the first figure, the link state database consists of five separate LSA's, one for each switch.

In switch A, there are 3 active interfaces, where B is connected to switch B with a cost of 4, then C is connected to switch C with a cost of 3 and E is connected to switch E with a cost of 1. Each switches will be indicated by the connection lines and then it receives and stores these five LSA's where Switch A provides services for application 1.The other field consist of sequence number, age of the LSA and checksum of the advertisement's contents.

Now the algorithm will start by setting the candidate list empty and putting the calculation of a switch on the shortest path set. After that it will get iterates and at each iteration, the shortest path set is examined by adding the switch. Then the steps are executed.

The candidate set (if they are not there already) is added with the switch X neighbours which is not belonging to the shortest-path set ; If the path through Switch X is shorter than the previously known path (if any) then the neighbours candidate paths are updated.

If the candidate list is empty, the algorithm terminates. The switch in the candidate set that is closest to the calculating switch is moved to the shortest-path set, and the algorithm iterates again.

In this diagram, the Dijiktra's calculation [5] in switch A would run.

- Initial state: The shortest path set consists of switch A itself and the candidate set is empty.
- Iteration 1: Switches W, X, and Z are added to the candidate set, and Z is then moved to the shortest-path set.
- Iteration 2: Switch Y is added to the candidate set, and Switch X's candidate path is changed to go through Switch Z. Switch X is then moved to the shortest- path set.
- Iteration 3: Switch W is moved to the shortest- path set.
- Iteration 4 : Switch Y is moved to the shortest-path set. The algorithm then terminates

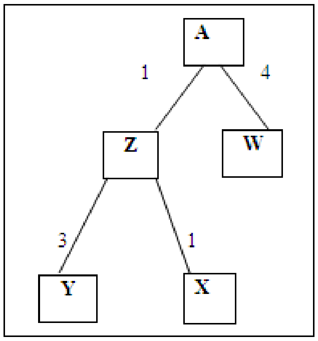


Figure 5: The Shortest Path Tree Calculated By Switch A, With A's Resulting Hop-By-Hop Routing Table

Destination	Next Hop	Cost
A	*	*
W	W	4
X	Z	2
Y	Z	4
Z	Z	1

Table 1

6.Attacks On TMP

6.1.Types Of Routing Attacks

Security has become the forefront of network management and implementation. Routing was an essential service for enabling communication in wireless sensor network and therefore potentially he target of many types of routing attacks. Karlof and Wagner [9] and others have systematically studied attacks on routing protocols. Those attacks are given below.

- Routing state corruption:
  It can be done by spoofing, altering, modifying or replaying routing information, the attackers were able to create routing loops, that increase end-to-end delay.
- Sleep derivation attacks:
  It increases the energy expenditure of sensor nodes and reduce the lifetime of the sensor network.
- Snooze attack:
  It result inadequate sensing coverage.
- Network substitution:
  Multiple attackers a collude to take control of part of sensor network.
- Wormholes:
  An adversary tunnels messages received in one part of the network over a low latency link and replays them elsewhere.
- Black holes:
  An adversary or compromised node lures nearly all the traffic from a particular area through itself, where the messages were dropped.
- Selective forwarding:
  Attackers selectively forward packets instead of faithfully forwarding all received packets or completely dropping all packets.
- Sybil attack:
  A malicious node behaves that it was a large number of nodes by impersonating the other nodes.
- Denial of Service:
  Most attacks result in a denial of service, but it's reserved for attacks that waste resources or disrupt service in a way that exceeds the effort required by an attacker. Ex: Message amplification and jamming.
- Hello floods:
  An attacker convinces nodes in the network that the attacker was a neighbour by broadcasting HELLO messages with high energy.

6.2.Attacker Classification

In Wireless sensor network there are a variety of attacks were possible. Those security attacks can be classified according to different criteria, such as domain of the attackers, or the techniques used in the attacks. These types of attacks [22] and all other networks can be classified into four criteria's. They are

- Laptop-class versus node-class attackers:
- Outsider versus insider attackers:
- Passive and active attackers:
- Cryptography and non-cryptography attacks:

6.2.1.Laptop-Class Versus Node-Class Attackers

A Laptop-class attacker uses a powerful device as compared to a sensor node. An attacker with these capabilities have access to greater battery, storage and computational resources than a typical sensor node.

A node-class attackers uses one or more devices with the same capabilities as legitimate sensor nodes. Therefore, it's only able to listen to or transmit messages within a limited range, and it faces constraints such as limited battery, small memory and a slow CPU.

6.2.2.Outsider Versus Insider Attackers

An outsider attacker has no knowledge of the protocols that were used in the network. But an insider attacker knows all information and knowledge of the protocol in the network, such as its cryptographic keys.

6.2.3.Passive And Active Attackers

Passive attackers do not involve in any alteration of data so it was difficult to detect. The message was transmitted in normal fashion but neither the receiver nor the sender was aware that a third party have observed the traffic pattern.

Active attackers involve in some modification of messages or data. It can be divided into four categories. They are Masquerade, replay, modification of messages, and denial of service.

6.2.4.Cryptography And Non-Cryptography Attacks

Some attacks are cryptographic primitive related and some of them are non- cryptography attacks.

Cryptographic Primitive Attacks

Cryptographic Primitive Attacks	**Examples**
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV)
Digital signature attack	RSA signature, digital signature standard
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128,RIPEMD

Table 2

7.A Brief Review Of Meta-TMP Protocol

Meta-protocol (Meta-TMP) is used to represent the topology maintenance protocols. There are different types of malicious behaviours and actions that can be carried out to attack a wireless sensor network. The countermeasures are used to increase the robustness of the protocols and make them resilient to such attacks. It includes an authentication mechanism that can be used to prevent outsider and certain insider attackers. Karlof and Wagner [9] describe the snooze attack to reduce the sensing coverage, against GAF, SPAN, CEC, and AFECA. The Meta- TMP[23] provides us with a better understanding of how a specific TMP works in the network and it acts as an efficient and useful tool for studying the security vulnerabilities of a specific TMP.

The TMP collects the nodes and exchanges the data with the neighbourhood and decides whether to be active or to be asleep. Here, Testing data is assigned to the data that each node needs to decide in which state of activity it should be in. Let each node collect the testing data in any state of activity..

The nature of the tests and its data type which is carried out by each node are similar to the characteristics and design of the TMP. It will decide the state of activity, density of active nodes, the position of the nodes, communication traffic of the neighbours, packet losing ratio, external environmental conditions and time. As a rule the node exchanges the data among other nodes by using unicast node-node, broadband node-neighbours, or eavesdropping on the neighbours.

Each node in TMP can be in one of the following states.

7.1.M-Test B

The starting state of each node. The node executes the Test B (Test Begin), and makes transition. If condition M-CB-S (Meta-Condition from Begin to Sleeping) is true, the nodes goes in to M-Sleeping state, but if the condition is false then it automatically goes in to Meta-Working state.

7.2.M-Sleeping

Here the nodes saves energy. If the M-EAWAKE (Meta Event Awake) occurs then the node goes into M-Testw (Meta Test Working state).

7.3.M-Test W

The testing state to start working. The node executes the Test w (Test Working), and makes transition. If condition M-CS-w (Meta-Condition from Sleeping to Working) is true, the nodes goes in to M-Working state, but if the condition is false then it automatically goes in to Meta-Sleeping state.

7.4.M-Working

If the M-EREST (Meta Event Rest) occurs then the node goes into M-Tests (Meta Test Sleeping state).

7.5.M-Test S

The testing state to go to sleep. The node executes the Test s (Test Sleeping), and makes transition. If condition M-Cw-s (Meta-Condition from Working to Sleeping) is true, the nodes goes in to M-Sleeping state, but if the condition is false then it automatically goes in to Meta-Working state.

Then when the battery runs out or when the node fails, then only the node reaches the "Meta-TMP Stops" state. Thus the communication pattern used by TMP plays an important role in network security.

8.Future Enhancement

The future Internet will need to be more intelligent and adaptive ,optimizing continuously the use of its resources and recovering from transient problems ,faults, and attacks without any impact on the demanding services and applications running over it. The research challenges associated with the proposed paradigm will be widely addressed and relevant in network management functionality will become a reality in the medium to long term. As part of our future work the basic Meta-TMP protocol has low density, but for practical system it need high density deployments as evaluated in this paper, for power management, reliability and sensing coverage. Thus the future studies could evaluate density to fully explore the behaviour for Meta-TMP protocol. Most of the mechanisms that have been proposed for broadcast authentication would appear to be more expensive. Thus, further research is necessary to develop efficient mechanisms for all kinds of broadcast in sensor networks.

9.Conclusion

In this article, the concept of shortest path routing on overall network performance was described. The Border Gateway Protocol (BGP) plays a vital role in order to determine the optimal routing path and the transport of information groups i.e, packets through an internetwork without the cause of packet loss, delay variation, delay of time and throughput of messages. BGP solves serious problems and it performs routing between multiple autonomous systems or domains and exchanges routing and reachability information with other BGP systems. The SPF (Shortest Path First) algorithm is used to find the shortest path that reaches the destination nodes from the source without any traffic. Routing calculations are also solved for shortest path routing determination. This research helps to develop efficient mechanisms to local broadcast authentication in sensor networks. The Meta-TMP is designed to a node to makes its own state transition decision and the state transition decision are revisited periodically. Finally the main conclusion is that selection of shortest path routing in network services and finding the distance is done by Border Gateway Protocol (BGP) by using SPF algorithm and routing calculations and authentication mechanisms are also included in the routing path and prevents all kinds of attacks by using Meta-TMP protocol in the network services which acts as an effective tool for traffic engineering.

10.References

1. R. Cohen and G.Nakibly, " On the computational complexity and effectiveness of N-hub shortest path routing," in Proc.IEEE INFOCOM, Hong Kong, March.2004.
2. A.Srinivasan, Approximation algorithms via Randomized Rounding: A Survey Lectures on Approximation algorithms and Randomized Algorithm. Wars Approximation algorithms via Randomized Rounding:Warzawa, PWN; Polish scientific,1999.
3. IEEE transactions on networking.
4. Computer Networks and Information Technology, International conference papers on advance in communication, networking and computing, springer.
5. Martha Steenstrub, " Routing in communication networks".
6. D.Awduche et al., Overview and principles of traffic engineering, IETF RFC,3272,May 2002.
7. B. Li et al., " On the optimal placement of Web proxies in the internet," in Proc. IEEE INFOCOM. New York, March 1999.
8. A.Gabrielli,L.V.Mancini, S.Setia, and S.Jajodia, "Securing topology maintenance protocols for sensor networks: Attacks and countermeasures," proc. First IEEE Int'l Conf.Security and privacy for emerging Areas in comm.. n/w, Sept 2005.
9. C. Karlof, N.Sastry and D.Wagner, "Tinysec: A Link layer Security Architecture for Wireless sensor network,"proc. Second ACM conf.Embedded networked Sensor systems,Nov 2004.
10. Teodor-Grigore lupu, "Main types of attacks in Wireless sensor networks", Dept. of computer and software eng., vasile Parvan 2,Timisoara.
11. Taka Miuguchi, Tomoya Yosghida," BGP route Hijacking", APRICOT,2007.
12. Ehab Al-sheer, "Network security attacks I: DDOS", Depaul university, 2007
13. Wiiliams stallings, "Cryptography and network security principles and practices," Fourth edition, Prientice Hall, 2005.
14. Saoud Sarwar, Deepa Mahra," Optimization of Computer network," IJSCE publications, IP university, New Delhi.
15. C. Karlof, and D.Wagner "Secure routing in wireless sensor network: Attacks and countermeasures". In first IEEE International Workshop on sensor network protocols and applications. Pages 1-15,May 2003.
16. A.Perrig, et al., "SPINS :Security protocols for sensor networks" In proceedings of seventh annual international conference on Mobile computing and network, MOBICOM 2001 Pages-189-199, july 2001.
17. M.G. zapata and N.Asokan, Securing and hoc routing protocols. In Proc. ACM workshop on wireless security, pages 1-10, ACM Press,2002.
18. L. zhou and J.Haas. "Securing and hoc networks" IEEE network,13(6):24-30,1999.

19. S.Choi and Y.Shavit,” Proxy location problems and their generalizations,” in Proc. Int. Workshop New Advances of web server and proxy technologies, Providence, RI,May 2003,pages 898-904.
20. S.Jamin et al., “Constrained mirror placement on the internet,” in Proc.IEEE INFOCOM, Anchorage, AK,Apr.2001,pp 31-40.
21. U.Srivastava et al.” Operator placement for in-network stream query processing” in proc. VLDB,Toronto,Canada, Aug- sep 2004, vol.30,pp 456-467.
22. Anthony D.Wood,Lei fang, Dept of computer sci.,” SIGF: A family of configurable, Secure routing protocols for wireless sensoe networks”.
23. Andrea Gabrielli et al., “Securing topology maintenance protocols for sensor networks” IEEE ,Vol 8, no 3 May/june 2011.