Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Study on Protection and Recovery mechanism in case of Network Failure

Safia Fatima[1]
[1]ResearchScholar
JJT University Jhunjhunu Rajasthan India
Assistant Professor, K.C.T.E.C. Gulbarga Karnataka 585103
India

Dr. Abdul Waheed[2]
[2] Associate Professor,
VTU Regional Office,
Gulbarga,Karnataka 585103
India

Abstract: - This paper discusses the survivability mechanism of a network; we propose a mechanism which would work on real time network environment based on division of recovery mechanism into protection switching and restoration mechanism. The network employs the split and merge mechanism for the transfer and reception of data. The main objective of this paper is to study and analyze the security problem of the data as well as reliability of the network to ensure safe and quick transmission of data even in the case of network failure.

In this approach the existing multipath rating algorithm is compared with Advanced Encryption Standard (AES) Algorithm and the Wireless Security Networks discussed by taking the Authentication and Encryption process for Bluetooth. The recovery mechanism explores all the network topologies and the mechanism necessary to recover the data in case of network failure. Recovery mechanism provides a more reliable way of data transmission over a dynamic and adaptive network while maintaining Data Integrity.

Keywords: Wireless Sensor Networks (WSN), Advanced Encryption Standard (AES), Self-healing Network (SHN)

I. Components of Wireless Sensor Networks:

There are three main components in wireless sensor network. They are

- Sensor
- Processor
- Radio for wireless communication

a. Sensors: Sensors will be having wireless communication capability for processing the signal as well as networking the data. They are the devices that provide us a measured response whenever there are changes that happen in its working environment. Sensors mainly measures physical data that is to be observed. Whatever the analog signals formed because of the sensors will be then converted to digital form by using the analog-to-digital convertor and then will be further processed.

b. Processor: Processor acts as an intermediary between radio as well as sensors. All the communication that happens between radio and sensors happens with the help of processors. We also do have a timer coprocessor, which is used for scheduling.

II. Node Evaluation

a. Power: So as to convene the application necessities the single sensor nodes have to consume extremely less power. Unlike I cell phones which consumes maximum power consumption which will be measured in hundreds of milliamps, the average power consumption must also be measured in micro amps. For achieving the low power operation we need to combine short power hardware elements as well as short function cycle process methods.

b. Flexibility: Whenever we have designed the application for a wide range of scenarios then it does mean that node architecture must be quite flexible as well as adaptive. This is mainly because a different application requires different lifetime, response time as well as response time. This is why sensor net set up structural design should be stretchy sufficient to put up an extensive vary of software actions. The architecture must also be easily implemented by using merely the correct group of software and hardware elements.

c. Robustness: Whatever the application that is designed must support lifetime requirements, so each node in the network must robust. In case of typical working environment, hundreds of nodes need to work together for many years. So for achieving this, the application has to be composed such which it could endure as well as settle in to the individual network machine breakdown.

For developing a robust system, system modularity is the powerful tool. By dividing the functionalities keen on remote sub-pieces every task could be completely examined taken them in separation and then uniting them into an absolute software. So as to make possible this, the application elements must be as autonomous as likely as well as should contain interfaces which are slender. Since the wireless sensor networks co-exist through additional wireless methods, they require to adapt as per that. The heftiness of these wireless connections to the exterior intrusion could be really augmented with the use of multi-channel and can be spread across the network (X. Y. Li, K. Moaveninejad, and O. Frieder, 2005).

d. Security: In order to meet the software phase safety, individual network machines has to be proficient enough to perform the complex encrypting as well as decrypting. Usually in case of wireless sensor networks, it will be easily susceptible to interception. So the only means of keeping the networks private as well as authenticated is encrypting the data transmissions.

Not only should the sensor networks should provide security for the data that is transmitted through its node but also must be capable of providing security to the data that exist with it. Even though the sensor nodes will not be having huge quantity of software to be preserved inside, they need to preserve clandestine encryption keys. If the keys are revealed, then the security will crumble.

e. Security Analysis: The transmission of tuple Q to the receiver via a secure channel ensures the confidentiality of the message. However, tuple R can be communicated through open channel. So, R becomes easily accessible. And if the value of R is known it becomes very easy for the intruder to decode the data, in this manner this method creates a bleach for security of data and a single point of failure in security for this reason we propose an architecture in which the encoded data is encrypted using Advanced encryption stand algorithm which helps us in increasing the security.

III. Methodology of the Research:

The proposed system which follows sensor technology is one with better, as well as cheaper technology which makes use of sensors which can be used both in civilian as well as military applications. This can mainly be used in environments which is very harsh, unreliable or few times adversarial. Under such circumstances we deploy large number of sensors which helps in achieving high quality.

On another hand sensors mainly communicate with wireless sensor networks which have the network bandwidth less than wired communication. The above mentioned issues will bring new design to the DWSN (Distributed Wireless Sensor Networks).

a. Topologies

There are several net topologies which are relevant to WSNs.

1. Star Network

A star net setup is communication structure in which we have only one base station which is able to transmit and obtain the messages from numerous machines.

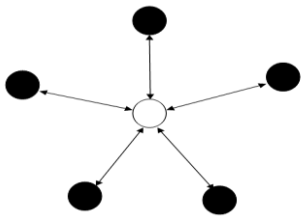

Figure 1: The architecture of Star network

2. Mesh Network:

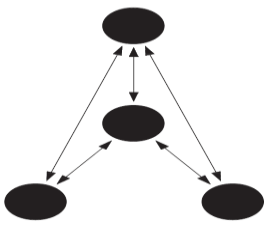

Figure 2: Mesh Network

In case of mesh topology, any node can transmit the data to any other node in the network. This particular type of transmission of data is known as multi-hop communication

3. Hybrid Star – Mesh Network

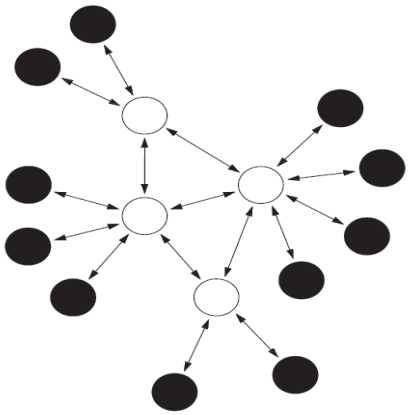

Figure 3: Hybrid Star – Mesh Network

It is one of the robust and versatile communication network methodologies, which helps in maintaining the wireless sensor network machines power utilization should be minimum. Here the added nodes on the net set up will be facilitated to have multi-hop capability which helps in forwarding the notification from short power nodes to the added nodes on the net set up. Usually the network machines by means of the multi-hop potential will be having elevated power.

IV. Attacks on WSNs

Whenever the user is using a wireless sensor network, there will numerous security threats which we face. In this project we are mainly concentrating on combating two such threats:

- Compromised-node(CN) assault
- Denial-of-service (DOS) assault.

The Compromised-node assault is a condition where in an opponent has a separation of network machines for eavesdropping the data whenever it is transmitted. In case of Denial-of-service attack, adversary mainly interferes with the normal operation by changing the functionality of subset of nodes, disrupting the functionality and so on. These two types of attacks are almost similar since they both generate black holes. A black hole is the area within which the adversary can disrupt the nodes actively or block the information from transmitting. Since the wireless sensor networks are incapable from stopping generating the black holes, whenever there is severe CN attack or DOS attack, these black holes disrupts normal data delivery between the nodes (P. Papadimitratos et al., 2006).

The traditional cryptographic methodologies alone can't provide solutions to any of the problems like this. This is due to the fact that, one if at all if the nodes are compromised; the adversary can always capable of acquiring either the encryption/decryption keys of particular node. Along with that, the adversary can also perform some type of DOS attack even though if it doesn't have the knowledge of the cryptosystems which are used in the wireless sensor network.

For encountering this problem, one of the available solutions is exploiting the network's routing functionality. If we can get to know the black holes locations in prior, then information can be sent over that node which doesn't have the black holes. Practically, since there is a problem in acquiring the location details, the above will be applied in a potentiality manner

An information in the form of packets will be broken into several shares (M) i.e. components which carry partial information by using mechanisms such as threshold secret sharing mechanism. Here we can acquire the original information by combining the T shares, but not less than the T shares. But in this above approach, there will be several security related issues. The main problem is that this approach will not be better option if at all if the adversary is capable of compromising or jam the nodes.

This is due to the fact that for the multiple routing algorithms, there will always be a fixed set of routes or paths. Due to this, even if at all if the shares are distributed over the network, and even if they traverse through different path, but they will always be delivered over same set of routes. So once the adversary gets to know about the routing algorithm, the adversary can then calculate the group of routes for whichever of the specified source and destination. During such circumstances, the challenger is able to pin-point to any of the one node and compromises those nodes. Secondly, since there will be only few no network machines-disjoint ways which could be established among source and destination. The main problem is that since the routes are calculated in some restrictions, the routes might not be spatially being dispersive enough for circumventing the black-hole (P. C. Lee et al., 2005).

In this project, we mainly explore the potential for random dispersion of information in case of wireless sensor networks. Here, conditional on the information kind which is obtainable to sensor, 4 shared plans will be generated in favour of broadcasting information. The four different schemes are:

1. purely random propagation
2. Non –recurring random broadcast
3. Multicast tree aided random broadcast.
4. Directed random propagation.

The PRP works by utilizing merely single hop area information as well as then furnishes the baseline information. The DRP methodology uses two-area data and provides the baseline performance. In case of MTRP it propagates shares or packets of information in the way of sink, thus creating the complete release procedure power competent.

V. Proposed System

a. Architecture

In this proposed system we propose that the encoded data that has been compressed using Mod-encoding is encrypted using AES algorithm (Farina, A et al, 2008) which is a strong symmetric key algorithm where the algorithm is presented below-

b. High-level description of the Algorithm

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule
2. Initial Round AddRoundKey—each byte of the state is combined with the round key using bitwise xor
3. Rounds
   - 3.1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - 3.2. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
   - 3.3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
   - 3.4. AddRounbdKey
4. Final Round (no Mix Columns)
   - 4.1. Sub Bytes
   - 4.2. Shift Rows
   - 4.3. AddRoundKey.

The process flow of encoded encryption data is shown using the following process flow diagram

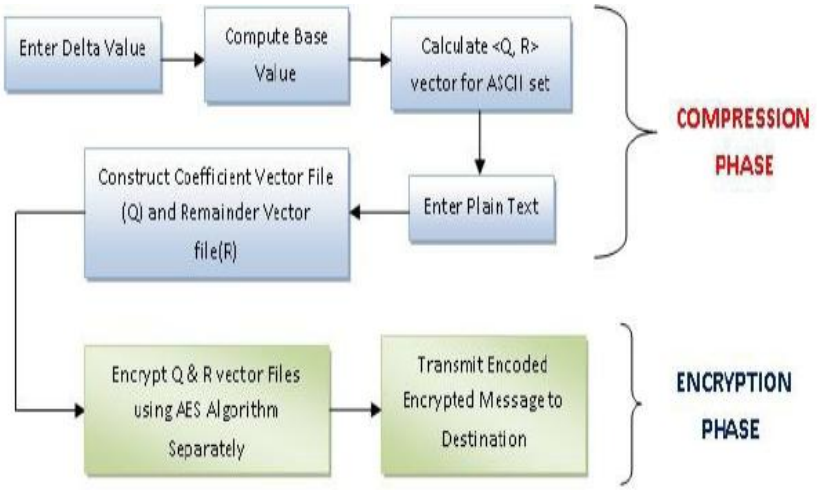

Figure 4: process flow for encoded encryption

In the Fig. 4 we have two phases compression phase and encryption phase. In compression phase we use Mod- encoding technique which was already discussed above in the compression implementation section [1]. As the process flow states, we enter the delta value which helps to calculate the base value by using the formula (256/delta)+1, using the obtained base value we generate <Q,R> vector for ASCII set. Using this <Q, R> vector we encode the plain text into encoded data which ensures our compression. In the encryption phase we encrypt the obtained Quotient (Q) vector compressed file as well as Reminder(R) compressed file using AES algorithm which was already discussed above. Hence the compressed(encoded), encrypted file is sent to the Destination which ensures our security while passing the data through an public channel, the data received at the destination is decrypted decoded same as the above said components in the backward direction as shown in the Fig. 4.

c. Security Prospective

When the security issues of existing system with encoding [1] is compared with the proposed system, we identify level of security increase in the proposed system which gives us integrity to the compressed data which adds us double security to the data which is passed through an unsecured channel.

VI. The encryption algorithm in Bluetooth security mechanism

a. Authentication and encryption process of Bluetooth

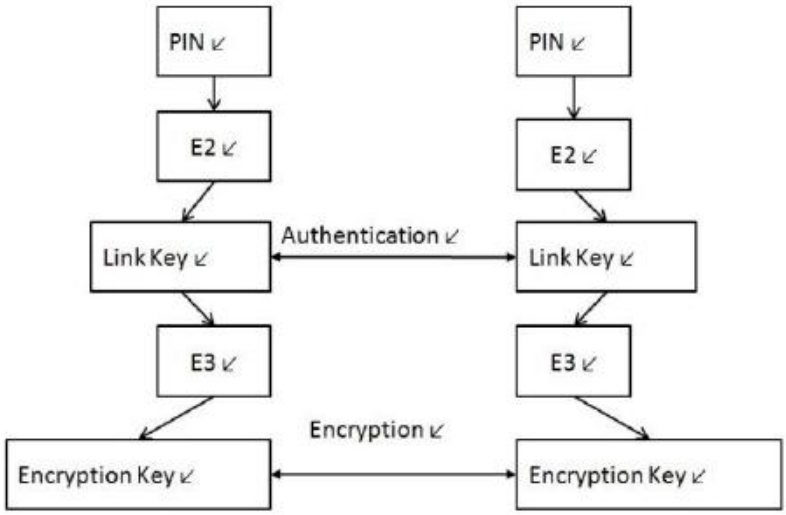

Figure 5: encryption process of Bluetooth

Bluetooth security-mechanism is divided into three modules including key generation, authentication and encryption, and adopt four kinds of algorithms as E0 E1, E2, E3. Bluetooth system provides authentication, encryption and key management functions in Link layer. PIN code was entered by the user, by means of the E2 algorithm for generating the link key, by means of E3 algorithm, getting encryption key, make use of E0 algorithm generated key stream, and encrypt plaintext, then get cipher text. Fig. 5 is the process of Bluetooth encryption (M.Shnad et al, 1993).

b. Analysis of E0 Algorithms

E0 algorithm is the encryption algorithms in Bluetooth link layer, which belongs to stream encryption method, that is to say it take data flow and the key bit stream Exclusive-or operation. The payload of each packet is encrypted separately, and the encryption occurs before MPE-FEC, after the cyclic redundancy check. The main principle is to use linear feedback shift register to generate pseudo-random sequence, after that form key stream that can be used for encryption, and then take the key stream and data stream that need encryption Exclusive-or operation, and achieve encryption. During decryption, the cipher text take Exclusive-or operation once more, re-plaintext can be obtained.

c. Process of encryption

During the process of sending encrypted information, Triple DES, requires 168-bit key and encrypts each block three times. That is, each block of data is actually encrypted 48 times, it encrypt the plaintext to produce cipher text. On the other hand, the sender get debit's public key from public key management centre, and then using RSA to encrypt session key. Finally, the combination of the session key from RSA encryption and the cipher text from Triple DES encryption are sent out.

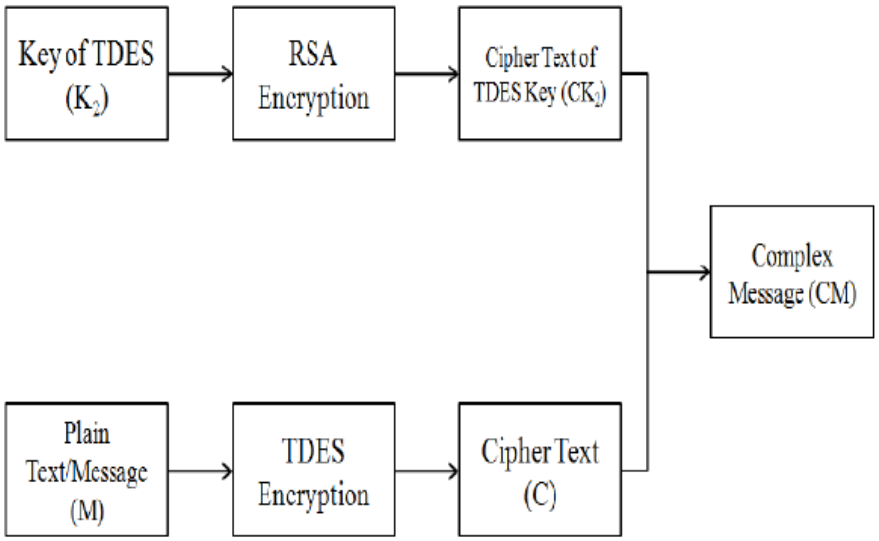

Figure 6: The whole mixed-encryption process.

d. Process of decryption

The decryption of hybrid encryption algorithm is as follows. The first, the receiver divide received cipher text CM into two parts, one is cipher text CK2 from the RSA algorithm encryption, and the other is cipher text C from the Triple DES algorithm encryption. The second, the receiver decrypt cipher text CK2 by their own private key dB, receive the key K2 which belongs TDES algorithm, then decrypt the cipher text C to the original M by keys K1, K2, K3. Figure 3 is a decryption of hybrid encryption algorithm (R.Rivest et al, 1978).

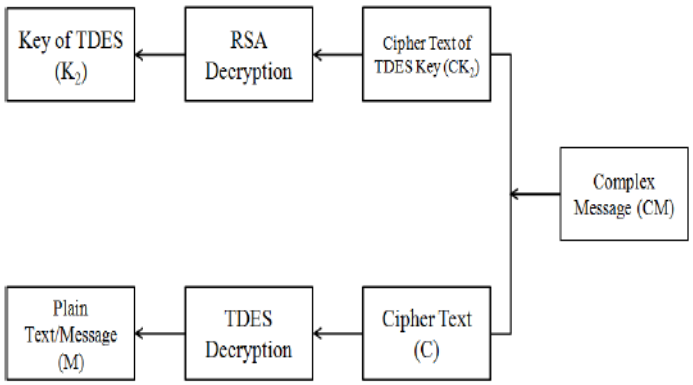

Figure 7: A decryption of hybrid encryption algorithm.

VII. Recovery Mechanisms

Several categorization schemes exist to classify network survivability mechanisms. The most common classification is to divide recovery mechanisms into protection switching and restoration mechanisms. Protection switching mechanisms use predefined alternative paths, while for restoration mechanisms alternative paths are calculated on demand after the detection of a failure. ATM recovery mechanisms are classified into protection switching, rerouting and self-healing mechanisms. Rerouting mechanisms are restoration mechanisms with centralized control, while distributed restoration mechanisms are called self-healing.

To use an unambiguous naming scheme in the recovery framework the recovery mechanisms are divided in protection switching, (distributed) restoration, reconfiguration (centralized restoration), and rerouting (at the service level). Figure 1 summarizes all options of the recovery framework. In this work the focus is set on protection switching and restoration mechanisms.

VIII. Recovery Model

a. Protection Switching

In the case of protection switching, an alternative connection is pre-established and pre-reserved (pre provisioned). Therefore, protection switching realizes the shortest disruption of the traffic, since no routing and resource allocation is required after failure detection. In the SDH standardization the maximum allowed switching time of protection switching mechanisms is defined to be 50ms. Depending on the recovery scope, the alternative connection is either switched at the source and target network element (global protection or path protection), or locally at the network element adjacent to the failure (local protection or link protection).

b. Dedicated Protection

In case of dedicated protection, the protection resources are used dedicatedly to the corresponding working connections. There are two dedicated protection schemes: 1+1 (one plus one) and 1:1 (one for one) protection. In Figure 2 both dedicated protection schemes are compared. The primary path is called working or active path (a). The secondary, alternative path is called protection or backup path (Autenrieth et al, 1998).

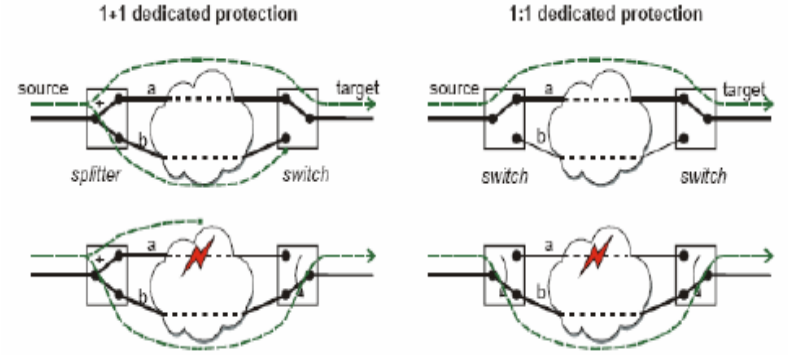

Figure 8: 1+1 and 1:1 protection switching

In 1+1 protection, the traffic is simultaneously transported over the working and protection path. In case of the failure, the target node only has to select the incoming traffic from the alternative path. With this combination, hitless recovery is possible. In several protocols for hitless switching are analysed. In case of 1:1 dedicated protection, the traffic is switched to the backup path V only after a failure is detected on the active path 'a'. Under normal conditions, the backup resources can be used for the transport of low-priority pre-emptive traffic, so-called extra traffic.

c. Shared Protection

With shared protection the spare resources are not dedicated for the recovery of a specific connection, but can be shared by multiple connections for different failure scenarios. Fig. 9 illustrates the concept of shared protection.

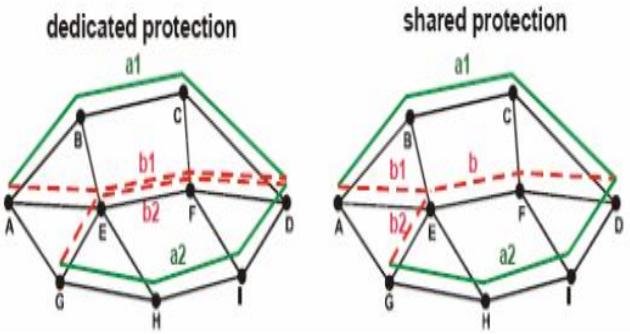

Figure 9: Dedicated and shared protection

On the link E-F the sum of the capacity of the two working connections A-B-C-D and G-H-I-D has to be reserved for the dedicated protection. In case of shared protection, only the larger capacity of A-B-C-D or G-HI-D has to be reserved. In connections with equal capacity C are used, dedicated protection requires 2 C spare resources on link E-F and 6 C spare resources altogether for the protection of the two connections. With shared protection, the required spare resources are 1 · C on the link E-F, and 4 · C for the full connections. Because of the sharing of the spare resource, shared protection has better resource efficiency than dedicated protection. On the other hand, it requires a more complex signalling mechanism for the activation of the alternative connection. Shared protection mechanisms are common for ring topologies, where the spare resources are provided by additional fibres used only for protection traffic and extra traffic (Autenrieth and Achim, 2002).

d. Restoration

In the case of restoration, an alternative path is calculated and established on-demand after the detection of a failure. Since the calculation of alternative routes and the signalling and resource reservation of a new connection are time-consuming, restoration mechanisms are considerably slower than protection mechanisms. There is several restoration mechanisms published, like the Self-healing Network (SHN), FITNESS, or RREACT. In general, restoration mechanisms search for a suitable backup path using distributed flooding mechanisms. Depending on the scope of the recovery mechanism, local or global, the node upstream of the failure or the source nodes of affected connections broadcast reservation messages on all outgoing links with enough spare capacity. When a broadcast message reaches the destination node, this node responds with an acknowledgement message (Grover, W.D. et al, 1998). Either the restoration is complete, when the acknowledgement message reaches the source node (2-phase algorithm), or the source node has to send a confirm message downstream to the destination node (3-phase algorithm).

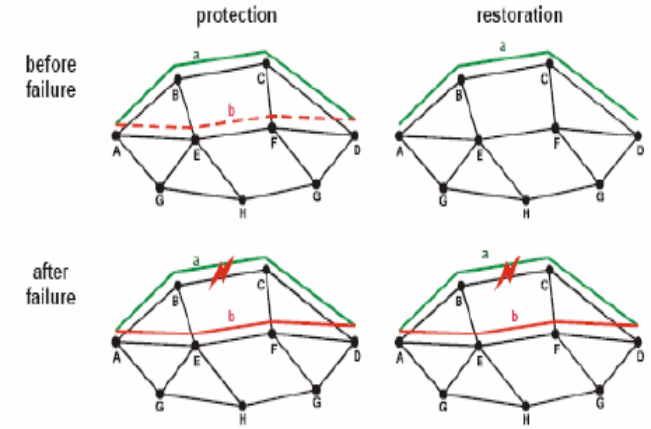

Figure 10: Protection and restoration

As an alternative to a flooding procedure, the upstream switching node can use a constraints based routing mechanism to calculate the full restoration route.

IX. Recovery Topology

The recovery mechanisms can operate in different network topologies. Ring networks are well suited for protection mechanisms, since they are the simplest form of a two-connected network.

One ring direction is used for the working traffic between source and destination, while the protection path is routed in opposite directions. In addition to two-fibre ring systems also four-fibre ring recovery mechanisms are possible. Protection mechanisms can also be used in mesh networks. Additionally, mesh network topologies also support restoration mechanisms. It was introduced the concept of p-cycles, which is based on protection cycles (overlay ring structure) working in a mesh network, utilizing the advantages of both, ring and mesh topologies. Fig. 11 illustrates the three recovery topology alternatives.

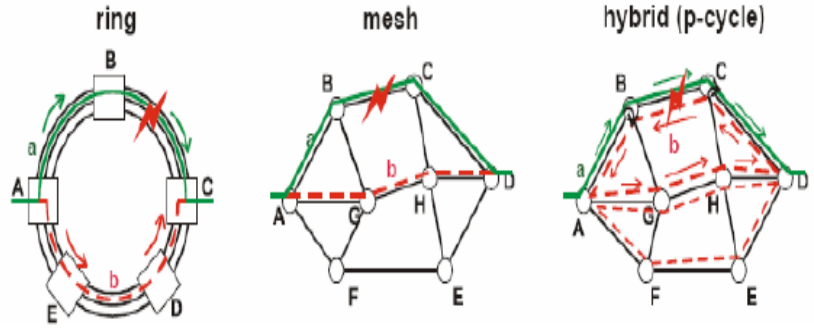

Figure 11: Recovery topology

e. Recovery Switching Operation Modes

Switching type: Unidirectional versus bidirectional switching

Two operation modes for recovery mechanisms exist for the recovery switching in case of failures affecting only one transmission direction. Such failures occur for example due to transmission laser outages. With unidirectional switching, only the affected direction of the failed traffic is recovered in case of unidirectional failures. In case of bidirectional switching, both, the affected and the unaffected direction of traffic affected by a unidirectional failure are recovered. For bidirectional switching, a protection switching protocol is required to control the switching operation. For ATM and SDH networks, this protection switching control protocol is called Automatic Protection Switching (APS) protocol. In case of unidirectional switching,

Only the sink node controls the switching operation, so no switching protocol is required. Therefore, unidirectional switching is less complex to implement and can operate faster. Unidirectional and bidirectional switching are also termed single ended vs. dual ended switching, respectively (Grover, W.D. 1987).

Fig. 12 illustrates the two switching modes.

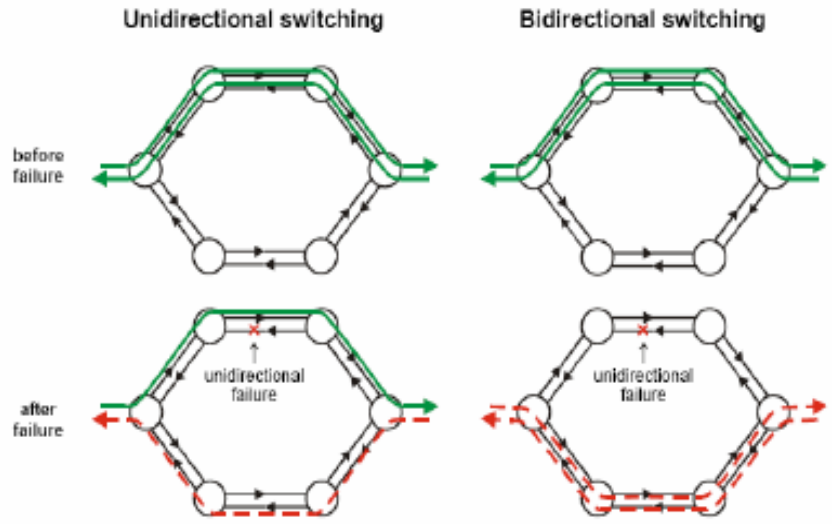

Figure 12: Unidirectional and bidirectional switching

X. ATM recovery mechanisms

The Asynchronous Transfer Mode (ATM) was defined as transmission technology for B-ISDN. Fig. 13 shows the reference model and the associated transport network layers. The reference model is divided in the physical layer, the ATM layer, an ATM adaptation layer and higher layers. For each layer a control plane and management plane is defined.

Figure 13: Relationship between virtual channel, virtual path and transmission path.

In this section the main characteristics of ATM protection switching and restoration mechanisms are presented, and the failure detection and signalling methods specified. The defect and failure detection and notification and the activation of recovery mechanisms in the ATM layer are realized using specific OAM (Operation, Administration, and Maintenance) cells. According to the five layers of the B-ISDN reference model, five hierarchical OAM flows F1 top F5 are defined are defined (Table 1).

OAM level	Network level	Network layer
F5	Virtual channel level	ATM layer
F4	Virtual path level	
F3	Transmission path level	Physical layer
F2	Digital section level	
F1	Regenerator section level	

Table 2: Shows the ATM OAM cells

XI. Conclusion

This paper proposes a unique method which uses the Recovery Mechanism of Protection switching and Restoration Mechanism in a real time network environment; the network uses the split and merge mechanism of Data transfer and Data Reception. The core focus of this paper is to study and analyse the security problem of the data as well as the reliability of the network to ensure safe and fast transmission of the data even in case the network fails.

Here we have also compared the multipath rating algorithm with Advanced Encryption Standard (AES) Algorithm and also the Wireless Security Network by taking the authentication and encryption process for Bluetooth. Recovery mechanism along with the network Topologies and Different Mechanism helps in recovering data when network fails. These Recovery methods provide a more reliable way of data transmission over dynamic and adaptive network for maintaining data integrity.

References

[1] Li X.Y, Moaveninejad K and Frieder O, (2005), "Regional gossip routing wireless ad hoc networks", ACM Journal of Mobile Networks and Applications, Volume : 10 No : 1-2, pp:61–77

[2] Papadimitratos P and Haas Z.J, (2002), "Secure routing for mobile ad hoc networks", In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS).

[3] Ross. A, (2001), "Security Engineering: A Guide to Building Dependable Distributed Systems", New York: John Wiley & Sons, Inc.

[4] Barrett.C. L, Eidenbenz.S. J, Kroc.L, Marathe.M and Smith.J. P (2003) "Parametric probabilistic sensor network routing", In Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA), pp. 122–131.

[5] Johnson.D. B, Maltz.D. A, and Broch.J (2001), "DSR: The dynamic source routing protocol for multihop wireless ad hoc networks" In C. E. Perkins, editor, Ad Hoc Networking,Addison-Wesley. pp. 139–172.

[6] Lou.W, Liu.W and Zhang.Y, (2006), "Performance optimization using multipath routing in mobile ad hoc and wireless sensor networks", In Combinatorial Optimization in Communication Networks, pp. 117–146.

[7] Papadimitratos P and Haas Z.J, (2003), "Secure Data Transmission in Mobile Ad Hoc Networks", ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA.

[8] Marina.M. K and Das.S. R, (Nov. 2001), "On-demand multipath distance vector routing in ad hoc networks", In Proceedings of the IEEE International Conference for Network Protocols (ICNP), pp. 14–23.

