ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

RESOURCE ALLOCATION FRAMEWORK FORWIRELESS NETWORK SYSTEMS USING DIFFIE HELLMAN ALGORITHM

Dr.H. Lilly Beaulah[1] , M.Jenolin Rex [2] and A. Amjath[3]

[1] Head CSE, [2]Assistant Professor, [3] PG Scholar

Department of Computer Science and Engineering, Mahendra College of Engineering, Salem

[1] ibeaulah@gmail.com, [2] jenolinrexm@gmahendracollege.com, [3]amjathjonh@gmail.com

Abstract:

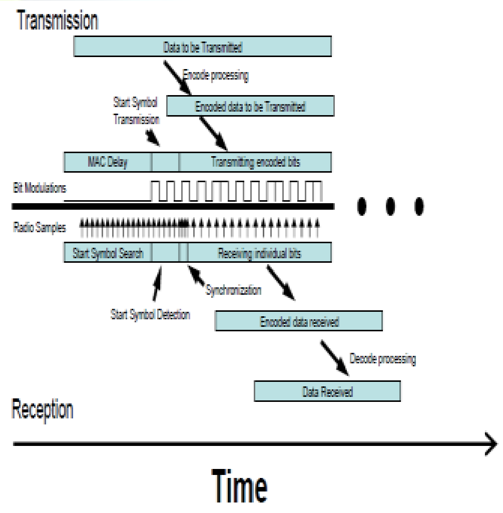
Distributed Time Sequence Routing protocol (DTSR); the DTSR is used to locate the correct relay node and sink node for data transmission. In our wireless network is considered in to neighbor's node in the network. Using the node data will be sending in to source to destination. To reduce the energy cost, nodes are active only during data transmission and the intersection of node creates a larger merged node. Then we recognize a particular set of sensor network applications so as to are flexible to this scalability limit. We are also improving the DTSR roaming with both network size and node density. The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys, whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme It enables that sensor nodes can communicate each other securely. The key distribution to sensor nodes is done by means of two layer process. This paper proposes a key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It based high level security and more energy efficient data transmission on their network.

1. INTRODUCTION

WN network are an emerging technology with a wide range of potential applications such as environment monitoring, earthquake detection, patient monitoring systems, etc. WN networks are also being deployed for many military applications, such as target tracking, surveillance, and security management. WN network typically consist of small, inexpensive, resource constrained devices hop wireless network. Each node, called a WN Node, has one WN, embedded processors, limited memory, and low-power radio, and is normally battery operated. Each WN node is responsible for sensing a desired event locally and for relaying a remote event sensed by other WN nodes so that the event is reported to the end user.

The main characteristics of a WN network include

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Unattended operation
- Power consumption.



Mobile stations are mounted upon public buses circulating within urban environments on fixed trajectories and near-periodic schedule. Namely, sinks motion is not controllable and their routes do not adapt upon specific WN network deployments. Our only assumption is that WN s is deployed in urban areas in proximity to public transportation vehicle routes. As a fair compromise between a small numbers which results in their rapid energy depletion and a large number which results in reduced data throughput. Finally, SNs are grouped in separate clusters. Raw WN y data are filtered within individual clusters exploiting their inherent spatial-temporal redundancy. Finally, we assume the unit disk model, which is the most common assumption in WN network literature. The underlying assumption in this model is that nodes which are closer than a certain distance can always communicate. However, in practice, a message sent by a node is received by the receiver with only certain probability even if the distance of the two nodes is smaller than the transmission range. [7] discussed about Enhancement of TCP Throughput using enhanced TCP Reno Scheme. Mobile Ad-Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread application in military and civilian communications.

Handling Routing Disruption in IP Network

As discussed above, in the recent world of internet it is become necessary that service should be with high availability, reliability and robustness. There is a large impact of unavailability off the network communication all the time due to failure of links. To achieve goal of recovering the flow of the network should be resumed as quickly as possible. Here discussed the various techniques of the IP network recovery and resumption of communication. A technique Multiple Routing Configurations (MRC). It gives surety that the node as well as link failures are fast recovered in failed IP network. MRC follows the principle of storing the additional information of routing in the routers. When there is the exposure of failure at some link the flow of data is instantaneously directed through the alternate output link. This technique is suitable for single link failure affairs for both link and nodes with the single mechanism instead of knowing the reason of failure. It is a connectionless technique and works on hop-by-hop forwarding. MRC forms network configuration for the backup with small set by using network mapping graph and links associated with it. By overall observations of simulations, MRC approaches performance of re-convergence of global Network with Failure (shaded region). b) Failure Handling with RTR

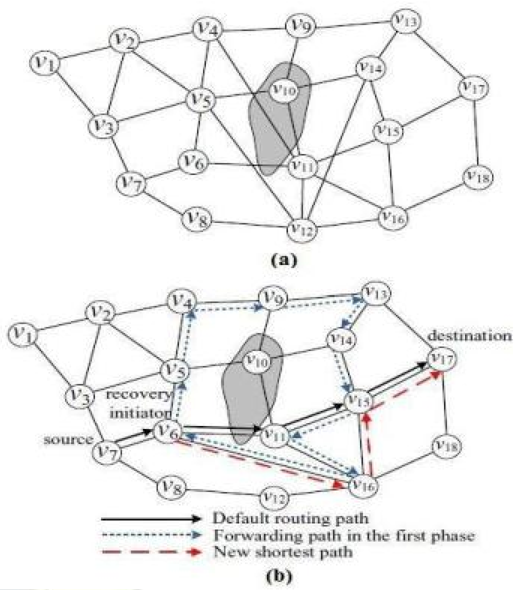


Fig. 1.2 a) network with failure (shaded region).
Fig. 1.2 b) failure handling with rtr

A technique called Reactive Two-phase Rerouting (RTR). This approach works for intra-domain routing failure recovery. The technique name suggests two phases, quick recovery from failures and finding the shortest recovery paths. Initial stage contains the collection of failure details by forwarding the packets in failed network. Second stage contains the finding out shortest path for the destination from the current source and packets are forwarded through that path. Network of any mapping can be handled by this technique for the recovering and finding shortest path up to destination. Simulation of this technique on the ISP topology shows that about 98.6% of failure paths are recovered with shortest path in the recovered network. As compared to previous techniques, network resources used for the irrecoverable paths of failed network is very less along with the better performance for recovering failed network. Proposes a mechanism for dual link failure recovery of networks. It works on the principle of re-routing of one failed link without knowledge of second failed link i.e. re-routing is independent of the other failed links. In this technique there are three protection addresses along with normal address for each node in the network and three protection graphs associated with them. In case of the protection graph, it is always two-edge connected with guarantee. In dual link failure the network is recovered from first failure by tunneling with the help of protection addresses and packet is routed.

Random link failure handling with the devoted backup network

This proposal leads to the conclusion that three protection addresses for each node are sufficient for the dual link failure recovery. A scheme for finding backup paths in advance effectively to minimize the response time. Backup paths are chosen for the optional disjoint flow of packets for the primary paths of the network. The backup paths are chosen by two cases first, for all the links in the network communication and second, for the links which are not protected or shared links. In the network all links are not equally vulnerable to the failure; even though it's not cost effective to provide full protection scheme for all the links. In this proposal such a cost-effective schemes are proposed like, CERNET2 to analyze the failures from the real world traces. Here the selective protection scheme is followed because the failure probabilities are heavy-tail means the failure occurs due to the small set of links. Matthew Johnston proposed a scheme for random link failure handling with the devoted backup network. After link failure in the network the traffic is diverted via pre-planned backup path. In finding out solution for the random link failures probabilistic survivability guarantees are provided to limit capacity over-provisioning. Here showed that the reliability of the primary network is gives stand to the optimal backup routing. In particular, when primary links becomes more failure resistant, the backup networks utilize optimally for additional resource sharing amongst available paths. Here the design and the capacity stipulation of the backup network are done based on the robust optimization.

Backup Network; Dotted Link: Primary Network proposes a model in which the disjoint path selection mechanism is used for the networks of Generalized Multi-Protocol Switching (GMPLS) by using the constraints of Shared Risk Link Group (SRLG). This scheme also called as the Weighted-SRLG. At the time of execution of the shortest path algorithm the numbers of SRLG members are treated as the link cost. A link which has less number of SRLG members is selected as the shortest path always instead of some rare cases. This scheme concludes with the WSRLG is best for selection of disjoint paths over the conventional shortest path algorithm. The model mentioning the provision for services at optical layer of the network. The problems in the constraints of static provision is handled and formulated in different conditions of resource availability. SRLG-diverse path protection schemes are applied in the three classes as dedicated, shared and unprotected. A light path length constraints and revenue value associated with it is associated for each connection request. In the unavailability of the sufficient resources the revenue maximization problem is

When the resources are sufficient the capacity minimization problem is formulated. A model in which developed various schemes of routing to deal with numerous correlated, failures. Recovery from multiple failures can't achieve by guarantee till single link failure handled with disjoint path protection. In case of disasters or intentional attacks recovery mechanism is not that simple. By considering probabilistic network failures diverse routes have found by minimum joint failure probability and developed a Probabilistic Shared Risk Link Group (PSRLG) framework for handling correlated failures. By this framework, two paths containing minimum joint failure probability found to achieve optimal solutions. As discussed above schemes in are based on the principle of independent logical link failure handling. Further schemes and are contains the failure handling of the links by shared risk link group mechanism.

Dynamic Security Access Control

Normally with in Mobile WN Networks, secure communication can take place only when there are no malicious nodes. If any malicious node is occurring within the network means, its throughput gets affected and high security cannot be achieved .As static based approach is not feasible for achieving full security; Dynamic based approach is combined in these architecture to determine whether source node is a threat or not based on the dynamic conditions in the network. Dynamic approach would use risk as an input to adapt itself for varying network conditions. Risk refers to how much or how little a source node could be trusted. The main aim is to build a security architecture that uses dynamic access control scheme to perform risk aware network security management.

A security Enforcement Facility is mainly used for policy enforcement and enables risk aware network access management. AEF analyses incoming traffic and determines the amount of risk associated with each source. Access from source to destination is allowed only when the risk is low, if the risk is high then access would be denied to destination and on the other hand it performs a security. The node which needs to transmit data packet has to pass through AEF for a security.

Mobile Wireless Sensor Networks (WN) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Along with these attacks, routing attacks have received extensive attention since it could cause the most devastating damage to WN Earlier there is binary and response decisions is considered. Binary responses may result in the unpredicted network division causing supplementary damages to the network infrastructure, and responses could lead to overcome this we move to the proposed system. The architecture diagram of the project is given below which describe the flow of the process. Here before a packet could be transmitted have to find shortest path and predict the intruder and should transmit the packet in a secure way.

Our protocol works under the assumption of mobile nodes which collaboratively support network operation. Network partitions can occur at any time and membership can change frequently. We define as group the set of nodes which can communicate through routes of one or more hops. Nodes in the same group must share the same group key to exchange routing control messages. We suppose that nodes run secure optimized link state routing protocol, a link state proactive routing protocol. Then, all nodes always know the number of nodes with which they can communicate. Besides, secure optimized link state routing protocol controls flooding with a mechanism called Multipoint Relays. In this mechanism, only nodes selected as MPR forward control messages. MPR nodes are selected by each node amongst the set of one hop neighbors, in a way to reach all two-hop neighbors. Also, nodes discover the approximately delay between its clocks in secure optimized link state routing protocol to avoid replay attacks. This information is used in our proposal to establish a weak synchronization on the network.

Global Dynamic Source Routing

It uses light weight hash codes for sign generation and verification, which greatly reduces the computational load as well as processing delay at each node without compromising security. But it also uses public key cryptography partly in the mutual authentication computational overhead. The routers are secure and well behaved. These solutions are not suitable for WNs, since the nodes play the dual role of receivers (and senders) of the traffic and routers for forwarding other node's traffic. Furthermore, exploiting these properties increase the resource usage, making multicast an easy tool for launching denial of service attacks on resource constrained WNs. In this paper, we propose extensions to Architecture, to provide multicast security in WNs.

2. EXISTING SYSTEM

In existing system move away without charitable any notice to its helpful nodes. It cause change in network topology, and therefore, it significantly degrade the performance of a steering protocol. Several direction-finding protocol studies are based on node lifetime and link lifetime. Upon a link failure in the primary network, traffic is rerouted through a preplanned path in the backup network. The approach for dealing with random guarantees are provided to limit capacity overprovisioning. The optimal backup routing strategy in this respect depends on the reliability of the primary network. Specifically, as primary links become less likely to fail, the optimal backup networks employ more resource sharing among backup paths. The results from the field of robust optimization to formulate an ILP for the design and capacity provisioning of these backup networks.

Disadvantage:

- The backup path identification time is too high.
- During data transmission data will be loss.
- Easily noise will be occur then attacker will attack node easier manner.
- So over all network performance is low.

3. PROPOSED SYSTEM

Distributed Time Sequence Routing protocol has used to send the data efficiently and quickly on to their network. In this algorithm to find out the correct node locate route as well as direct path in the network base on the time. DTSR protocol is to transfer the data in to without any modification. Availability parameters mean connectivity and functionality in the network management layer. Connectivity is the physical connectivity of network elements. Loss is the fraction of packets lost in transit from sender to target during a specific time interval, expressed in percentages. Have to improve the network throughput, Network delivery ratio, and availability, data loss. Consequently, the Diffie-Hellman algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are established between nodes. The steering metrics are evaluated in dissimilar literatures to indicate the significance and measuring purpose of frequent routing protocols. In absolute surveys all along with the classification of these metrics by means of their meticulous classifications are discuss in detail.

Architecture Diagram

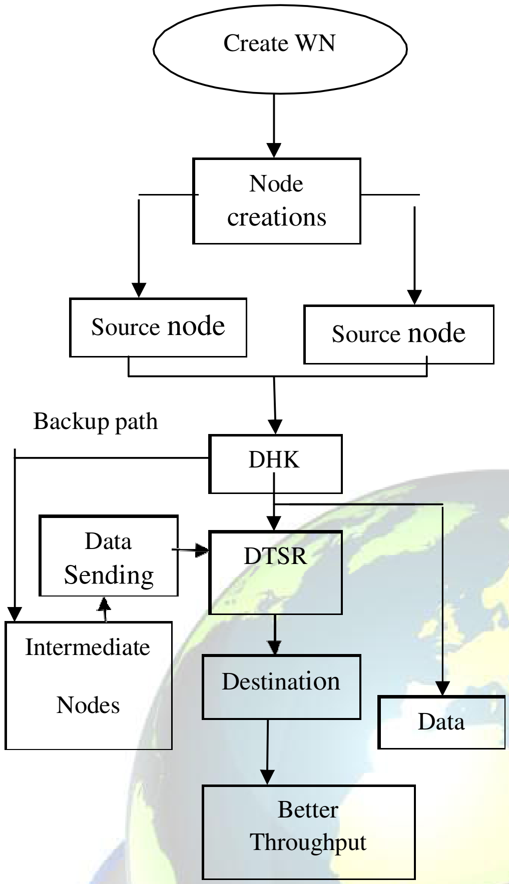


Fig.3 Architecture Diagram

Advantage

- It's used diffe hellman key so if any link failure means easily predict,
- Also backup identification is very easy
- Over all throughput is high so data will transfer without any noise.
- The packet delivery fraction is high
- So over all network perforce is high

4.MODULE'S DESCRIPTION

Wireless Channel Design

This module is developed to wireless network requirements, wireless equipment's, Transmitter and receiver between one to another node by calculate the distance. Wireless sensor transmission ranges cover all nodes.

Node Creating

This module is developed to node create more than 10 nodes placed at particular distance. Wireless node placed in intermediate area. Each access point has to receive, transmit packets and then send acknowledgement to transmitter.

Synchronization Of Multiple Nodes

Sensor networks most often have a much more complicated topology than the simple examples and not all sensor nodes can communicate with each other directly. Thus, multi-hop synchronization is required, which adds an additional layer of complexity. Clearly, this could be avoided by using an overlay network which provides virtual, single-hop communication from every sensor node to a single master node.

Diffie-Hellman Key Algorithm

It should be complemented with an authentication mechanism. In this approach for key distribution in security factors with respect fact that solving attacking problem is very challenging and that the shared key is never itself transmitted over the channel.

For example:

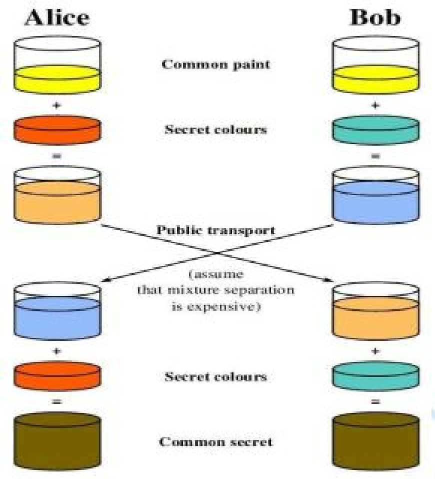


Fig.4.4 Diffie-Hellman key Exchange

Description:

Diffie–Hellman establishes a shared secret that can beused for secret communications while exchanging data over a public network. The following diagram illustratesthe general idea of the key exchange by using colors insteadof a very large number.

The crucial part of the process is that Alice and Bob exchange their secret colorsin a mix only. Finally this generates an identical keythat is computationally difficult (impossible for modern supercomputers to do in a reasonable amount of time) to reverse for another party that might have been listening in on them. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data. Note that the starting color

Alice and Bob. The starting color is assumed to be known to any eavesdropping opponent. It may even be public.

Cryptographic explanation

The simplest and the original implementation of the protocoluses the multiplicative group of integers modulo p, where p is prime, and a primitive root modulo p. Here is an example of the protocol, with non-secret values in blue, and secret values in **red**.

1. Alice and Bob agree to use a prime number p = 23
and base g = 5 (which is a primitive root modulo 23).
2. Alice chooses a secret integer ***a*** = **6**, then sends Bob
$A = ga \bmod p$
_ A = 5**6** mod 23 = 8
3. Bob chooses a secret integer ***b*** = **15**, then sends Alice
$B = gb \bmod p$
_ B = 5**15** mod 23 = 19
4. Alice computes ***s*** = B***a*** mod p
_ ***s*** = 19**6** mod 23 = **2**
5. Bob computes ***s*** = A***b*** mod p
_ ***s*** = 8**15** mod 23 = **2**
6. Alice and Bob now share a secret (the number**2**).

Both Alice and Bob have arrived at the same value, because $(ga)b$ (for Bob, 815 mod 23 = $(ga \bmod p)b \bmod p = (ga)b \bmod p$) and $(gb)a$ are equal mod p. Note that only a, b, and $(gab \bmod p = gba \bmod p)$ are kept secret. All the other values – p, g, $ga \bmod p$, and $gb \bmod p$ – are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them,for sending messages across the same open communications channel. Of course, much larger values of a, b, and p would be needed to make this example secure, since there are only 23 possible results of n mod 23. However, if p is a prime of at least 300 digits, and a and b are at least 100 digits long, then even the fastest modern computers cannot find a given only g, p, $gb \bmod p$ and $ga \bmod p$. The problem such a computer needs to solve is called the discrete logarithmproblem. The computation of $ga \bmod p$ is known as modular exponentiation and can be done efficiently evenfor large numbers. Note that g need not be large at all,and in practice is usually a small prime (like 2, 3, 5...) because primitive roots usually are quite numerous.

5. CONCLUSION

- Then the information based metric, entropy, is applied for final filtering of suspicious flow. Trust value for a client is assigned by the server based on the access pattern of the client and updated every time when the client contacts the server.
- It is a public-key cryptographic system whose sole reason is for distributing keys, whereby it is used to swap over a single piece of information, and anywhere the value obtained is in general used as a sitting key for a private-key system
- The proposed strategy is effective and efficiently scalable that has several advantages like memory non intensive, minimum overhead in terms of resources and time.

REFERENCES

[1].“Delay-Optimal Data Forwarding in Vehicular Sensor Networks”, Seokhyun Kim, Jaeseong Jeong-2013.

[2]. “VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks”, Jing Zhao and Guohong Cao.

[3]. “The Deployment of Multiple Infrastructures in Vehicular Networks”, Liu Shijia and Liu Shenghui.

[4]. “Advancing Geographic Routing in Vehicular Ad Hoc Urban Networks”, Kevin Lee and Mario Gerla.

[5]. “An evaluation of vehicular networks with real vehicular GPS traces”, Chao Chen and Min Gao.

[6]. “DAWN: A Density Adaptive Routing for Deadline-Based Data Collection in Vehicular Delay Tolerant Networks”, Qiao Fu, Bhaskar Krishnamachari.

[7]. Christo Ananth, Shivamurugan. C.,Ramasubbu. S, “Enhancement of TCP Throughput using enhanced TCP Reno Scheme”, International Journal Of Advanced Research Trends In Engineering And Technology (IJARTET), Volume II, Special Issue XXV, April 2015

[8]. “An Efficient Scalable Trajectory Based Forwarding Scheme for VANETs”, Houda Labiod, Nedal Ababneh.

[9]. “On Optimal Service Directory Selection in Urban Vehicular Networks”, Hongzi Zhu Jia-Liang Lu.

[10].“PMTR: Privacy-enhancing Multilayer Trajectory-based Routing Protocol for Vehicular ad hoc Networks”, Baber Aslam, Faisal Amjad.

[11].R. Koetter and F. Kschischang, “Coding for errors and erasures in
random network coding,” *IEEE Transactions on Information Theory*,vol. 54, no. 8, pp. 3579–3591, 2008.

[12].Y. Li and J. C. S. Lui, “Epidemic attacks in network-coding-enabledwireless mesh networks: Detection, identification, and evaluation,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 11, pp. 2219–2232 2013.