ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Security Based on Context – Aware Adaptive Routing in Delay Tolerant Mobile Ad Hoc Networks

[1]V. Anandkumar and [2]Dr.S.Subramanian

[1]*Assistant Professor, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, TamilNadu, India.*
[2]*Advisor, Coimbatore Institute of Engineering and Technology, Narasipuram, Coimbatore, TamilNadu, India.*

ARTICLE INFO

Article history:
Received 12 December 2014
Received in revised form 26 December 2014
Accepted 28 January 2015
Available online 1 April 2015

Keywords:
Mobile Systems, Security Issues, Ad Hoc Networks, Context Aware Routing Protocol, Delivery.

ABSTRACT

Applications that are not centralized in mobile systems are often characterized by partitions between networks which results in delay tolerant with multi stage security issues. It had received considerable attention to obviate to the gap between ad hoc network research and real applications. This paper gives the design, implementation and evaluation of the multi-stage security based Context-aware Routing (SCR) protocol for delay tolerant unicast communication in intermittently connected mobile ad hoc networks. The ultimate focus of the protocol is to utilize the nodes as carriers of messages among network partitions to attain quick delivery. With increase in security at each stage, the message in each node gets delayed to reach destination. So, the content aware procedure is followed to enhance the efficiency of packet delivery with security at multi-stage implemented.

To Cite This Article: V. Anandkumar and Dr.S.Subramanian., Security Based on Context – Aware Adaptive Routing in Delay Tolerant Mobile Ad Hoc Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(7): 669-676, 2015*

INTRODUCTION

At the new era of communication, the gigantic growth of mobile computing devices likely mobile and smart phones, Personal Digital Assistants (PDAs), and devices for accessing data such as wireless 2G or 3G modems etc. delivers the revolution in the computing world. Due to the faster growth in wireless network solutions, the security should be the key issue on (MANET) mobile Ad-Hoc network (Perkins, C.E., 2001). MANET is a system of wireless mobile nodes that dynamically self-organize and configured in arbitrary and temporary network topologies. People and vehicles can be connected with network in areas without a pre-existing communication infrastructure that requires extensions in wireless medium (Vahdat, A., D. Becker, 2000)[3]. The nodes can directly communicate with all the other nodes within their frequency limits in mobile ad hoc networks whereas nodes not in the direct communication range use intermediate node(s) to communicate with each other. In the above situations, all nodes have actively participated in the communication.

This paper provides the Security based Context-aware Routing (SCR) protocol to secure the node using delay tolerant mobile ad hoc network routing to allow the efficient secure routing of messages to the recipient. The main task of establishing a security for a node and a host willing to send a message to a recipient uses an SCR Filter probability based approach and multi-criteria decision theory to choose the best next hop for the message. The decision is based on the mobility of the node and its past collocation with the recipient. SCR does not assume any previous knowledge of the host routes as in other techniques such as the Ferrying of Messages which depend on the previous knowledge of the routes of the special hosts carrying the information. The implementation can be further extended by forecasting techniques for carrier culling founded on analytical probabilistic augury models.

Related Work:

Numerous techniques have been proposed to enable asynchronous articulation in intermittently connected mobile ad hoc networks. An approach was proposed to guarantee message transmission in minimal time. However, the algorithm relies on the fact that mobile hosts actively alter their trajectories to transmit messages. SCR has inspired the architecture of other protocols based on the study of mobility arrangements, where different behaviors for the estimation of host collocation were taken into consideration while selecting best carriers. The machine learning approaches were applied to extract

Corresponding Author: V.Anandkumar, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India.
E-mail: ak479940@gmail.com

social patterns among the individuals carrying the devices.

Issues In Existing Network Security Setup:

Delay-tolerant networking (DTN) is accessions to the computer network framework that address the technical issues in amalgamate networks reducing ceaseless network connectivity. Archetypes of such networks are those accomplishing in mobile or extreme worldwide environments, or networks arranged in space. Applications animus those demanding application DTN span in which the nodes (e.g., people and wild animals) move around in backdrops where frameworks cannot be protected for instance in case of emergency services, military demands and secured environments. Justifications for routing are presented for these cases, where the origin is from the basic contagious routing, which do not consider about the message storage and forwards them to all associated nodes, accomplishing a flood of communications. Routing protocols Ad Hoc On Demand Routing and Dynamic Source Routing take an "Accretion and Direct" mechanism, for iterative creation of data for caching them throughout the network so that it will finally reach its destination. A well known technique used to expose the anticipation of a message being transferred is to counterfeit many copies of the message in the hope that at least one will achieve in reaching its sink. This is suitable for networks with ample amounts of bounded source and inter-node bandwidth relative to the anticipated traffic.

We present the Security based Context-aware Adaptive Routing (SCR) protocol, an improvement to unicast communication mobile ad hoc network routing that uses conjecture to allow the effective routing of messages to the recipient. A host willing to send a message to a recipient uses a Kalman Filter conjecture and multi criteria decision hypothesis to choose the best next hop for the communication. The conclusion is based on the mobility of the host and its antecedent collocation with the receiver. SCR does not assume any previous knowledge of the hosts. Moreover, our protocol is based on a multiple replica of the message in the system, instead of having diversified clones.

A. Multistage Secure SCR Algorithm:

Variables

- Sec: multistage security
- $z(\tau)$: time series of residuals (conjecture errors)
- rk : autocorrelation coefficients
- k_{max}: max lag
- N: number of samples
- maxError: max acceptable conjecture error

```
Step 1: Boolean is probabilistic Predictable Secure
Sec( U (t-NT) … … U(t), Û(t- NT) … … Û(t)){
Step 2: for all Sec( τ ϵ [ t – nT, t ]) do
calculate z(τ)= Û(τ) - U(τ)
Step 3: for all k ϵ [1….. k_max] do
calculate rk of z(τ)
Step 4: if ((90% of {rk} ϵ [-2/√N, 2/√N]) and
(0.1z(t)<= maxError)) then
return true;
else
return false;
```

Where T is the number of connections and disconnections that a host experienced over the last T seconds, t is the time seconds is the utility function, Û is the utility function at t + T seconds. Fortunately, this conjecture problem can be expressed in the form of a state space model. Starting from a time series of observed values, a conjecture model based on an inner state is represented by a set of vectors. One of the main advantages of the Kalman filter was that it does not require the argosy of the entire past history of the system. It is suitable for a mobile setting in which memory resources may potentially be very limited. At the end of the paper, concepts of state space model to the analysis and the conjecture of context information were provided, discussing three cases according to the different behavior of the time series.

B. Architecture of the SCR Protocol:

B1. Protocol Architecture:

A comprehensive term that refers to a protocol, used by a router to determine the adapted path over which data was transmitted (Fall, K., 2003). The routing protocol also specifies how routers in a network accord information with each other. Routing protocols implement algorithms that tell routers the best paths through internetworks (Perkins, C.E. and P. Bhagwat, 1994). SCR routing protocol consists of basic ADHOC routing nature and calculation of probability transmittal module and its supported functions. Arbitrarily some values that were randomly distributed to each node are considered as the transmittal probability value of the node used for selection of advantageous hop.

B2. Structural Architecture:

The architecture for the routing process in an ad hoc network includes setting nodes, typical features (Number of nodes, nodes placement), motility process, counterfeit time, mac protocol etc..,

B3. Implementation of SCR Protocol:

Once the routing protocol is designed, some changes are made to transmit the messages from other layers in network supported layers (Jain, S., 2004). The routing protocol is implemented in the network layer of the layered architecture of the GloMoSim simulator.

B4. GUI Architecture:

Design the GUI phase to suite the routing process and measure it by some metrics like end to end delay, throughput, and collision, energy consumption by values and also by graph.

Proposed Scheme:

The main blueprint aim of SCR is to assist secure communication in intermittently connected mobile ad hoc networks. The key controversy solved by the SCR protocol is the selection of the carrier nodes. The elucidation is based on the appositeness of anticipating techniques and adequacy theory for the interpretation of various aspects of the system for taking defended routing decisions. SCR is able to deliver secure messages synchronously (i.e., without storing information inside buffers of intermediate nodes when there are no network partitions between sender and receiver). The transmission process depending on examining the node capability and various security analyses have been made to be sure as to whether or not the recipient is present in the same connected region of the network as the sender came from another secure arena or channel.

If both are in the same connected portion of the network, the message is transmitted using an underlying synchronous secure routing protocol to arbitrate a forwarding path. If a message cannot be delivered synchronously, the best defended carriers for a message are those that have the excessive chance of advantageous delivery, i.e., the highest secure delivery probabilities are computed to improve the effectiveness of secure path. The message is transmitted to the host with the excessive one using the underlying synchronous protocol. In order to understand the operation of the SCR protocol, consider the following scenario in which two groups of nodes are connected as in Figure 1.

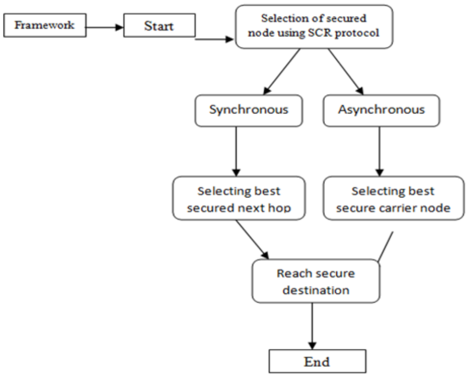

Framework
Start
Selection of secured node using SCR protocol
Synchronous
Asynchronous
Selecting best secured next hop
Selecting best secure carrier node
Reach secure destination
End

Fig. 1: Flowchart of the proposed scheme.

As given in the implementation, it was assumed that Dynamic Destination-Sequenced Distance-Vector [12] is used to support synchronous secure routing. Host A4 wishes to send a message to A8. This cannot be done synchronously, because there is no connected path between the two. Suppose the delivery probabilities for A8 are as shown in Figure 2(b). In this case, the host possessing the best transmission probability to host A8 is A5. Consequently, the message is transmitted to A5, which stores it.

During a certain period of time, A4 moves to the other network (as in Figure 2.b). Since a connected path between A4 and A8 now exists, the message is delivered to its intended recipient. Using DSDV, for example, A4 is able to transmit the message shortly after joining the network, as it will receive the routing information relating to A8. Delivery probabilities are synthesized locally from contextual information. We define context as the set of attributes that describe the aspects of the system that can be used to drive the process of message delivery. An example of context information can be the change rate of connectivity, i.e., the number of connections and disconnections that a host experienced over the last T seconds.

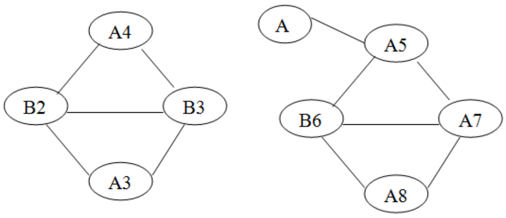


Fig. 2: Two connected networks, with associated delivery probabilities for message transmission between A4 and A8 (Fig. a).

This parameter measures relative mobility and, the probability that a host will encounter other hosts. Since it was assumed that every host at a certain time sends both the information related to the underlying synchronous routing (in DSDV this is the routing tables with distances, next hop host identifier, etc.), and a list containing its delivery probabilities for the other hosts. When a host receives this information, it updates its routing tables. With respect to the table to asynchronous routing, each host maintains a list of data, each of which is a tuple that includes the fields (destination, best Host, delivery Probability). A scenario was explored in which each message is placed with only a single carrier rather than with a set, with the consequence that there is only a single list entry for each destination. When a host is selected as a carrier and receives the message, it inserts it into a buffer. The size of this buffer is fundamental, and represents a trade-off between storage overhead and likely performance. If the buffer overflows, messages would be lost, since the existence of a multiple replica was assumed. In the following sections, the techniques were described for the calculation of the delivery probabilities.

Conjecture And Evaluation Of Context Information:

SCR is optimized by using assumed future values of the context attributes for making routing decisions, to have a more precise estimation of the time series associated to each context range (Kalman, R.E., 1960). For example, in the case of arrangements of collocation, a host HA, currently not collocated with a host HB may be considered of infrequent adequacy for acting as a carrier for HB if we estimate only this instant of time. However, HA may have been collocated with HB for the past three hours and, therefore, its contingency of being co located again, given the assumptions of the model, are high and should be represented accordingly. The process of conjecture and estimation of the context information can be summarized as follows.

- Each host computes its transmission probability for a given set of hosts. This method is based on the computation of utilities for each aspect describing the context. Then the future values of these utilities are conjectured and composed using multi-criteria decision theory in order to estimate the overall delivery probability. The computed delivery probability is systematically sent to another host connected as cloud (Kalman, R.E., 1960).
- Each host maintains a forwarding table of tuples describing the next analytical hop, and its associated delivery probability, for all known destinations.
- Each host uses local conjectures of transmission probabilities between updates of information. The conjecture is used during temporary disconnections and is carried out until certain accuracy can be guaranteed.

The architecture for the computation of the delivery probability that we designed for SCR is very generic and can be extended to any number of context aspects. In the rest of this section, the paper analyzes more closely how delivery probability information is conjecture, spread in the system, maintained, and evaluated.

Message Delivery:

A. Synchronous Delivery:

When a message has to be transmitted, if the recipient is reachable synchronously, it is advanced to the next hop indicated by nextHopId. This forwarding mechanism is the conventional one of distance vector protocols. It may happen that the path to a certain host is broken, but, at the same time, the routing table has not yet been updated with the information related to this change, given the procreation delay of routing tables. In this case, the message is advanced until it reaches the host that has been already notified about the disconnections. This host will then check if the message can be sent using the asynchronous delivery mechanism (i.e., an entry for the selection of the best carrier exists in its routing table). If not, the host stores the message in its buffer and tries to resend it periodically.

B. Asynchronous Delivery:

If a connected path to the recipient does not abide (i.e., the value of distance is equal or greater than 16), the message is forwarded to the host with the excessive value of delivery probability (expressed by delivery Prob). In order to reach the carrier, DSDV is used. In other words, the entry having the value of the key targetHostId equal to bestHopHostId is used to ahead the message. As the network is active, it may happen that the carrier is unreachable, since, in the meanwhile, it has left the connected network. In this case, if the information about the disconnection has attained the sender, the audit related to the best carrier is removed (set to an invalid state designated by 0). In order to avert the procreation of stale routes, we use sequence numbers for the routing tables like in DSDV. If this information has not been generated yet to the sender, the intermediate host acquainted of the topology change will try to resend the message.

C. Re-Transmissions:

Periodically, for each message in its buffer, a host checks its routing table. The message is then advanced simultaneously to the recipient or to a carrier if a corresponding entry is present in the routing table. If no entry is present, the message abides in the buffer. The number of there transmissions is another key configuration value that we have measured and tested during the performance evaluation of the protocol [17]. Each node also maintains a list of its adequacies for a certain set of hosts. In particular, each node keeps a list of the local adequacies related to the colocation with other hosts and one related to its change degree of connectivity. Periodically, these adequacies are composed and the resulting ones are checked against the utilities stored in the local routing table. If the adequacy of the host is higher of the one currently maintained in the table, the latter is replaced. The value of the adequacies is updated before allegorizing it with the entries of the local routing table.

Context Information Attributes Using Kalman Filter Conjecture Techniques:

Kalman filter conjecture techniques were originally developed in automatic control systems theory. These are essentially a function of discrete signal processing described by a state vector updated using a set of conjecture recursive equations. Kalman filter theory is used in SCR both to achieve a more realistic conjecture of the evolution of the ambience of a host and to optimize the bandwidth usage. As discussed above, the exchange of ambience information that allows the computation of delivery probabilities is a potentially expensive process, and unnecessarily so where such information is relatively predictable. If it is possible to conjecture future values of the attributes describing the ambience, we update the transmission probabilities stored in the routing tables, even if fresh information is unavailable (Kalman, R.E., 1960). Fortunately, this conjecture problem can be expressed in the form of a state space model.

Starting from a time series of noticed values that represent context information, a conjecture model is derived based on an inner state represented by a set of vectors. One of the main benefits of the Kalman filter is that it does not require the argosy of the entire past history of the system, making it suitable for a mobile setting in which memory resources may potentially be very limited. The paper also discusses how the Kalman filter model that are used in SCR can be amended and studied using alternative theoretical frameworks, namely EWMA, ARMA and Bayesian anticipating models.

A. Context Predictability:

The approach that we adopted is conjectured on the analysis of the time series representing the context information and, more specifically on residual analysis (Kalman, R.E., 1960). Given ascertain number of measurements of the predictability of the time series, we define predictability level of a context attribute as the percentage of samples for which the component returns true, in other words, the percentage of samples for which the conjecture model is sufficiently precise given a predefined acceptable fault.

Output Efficiency:

A. Packet Delivery Ratio:

The term is defined as the fraction of data packets transmitted to the sink those generated from a source. It can be simply stated as,

$$\text{Packet Delivery Ratio} = \frac{Destination}{Source}$$

Where, the destination represents the packet received at the sink whereas the source represents the packets generated at the source.

B. Average End – to – End Delivery:

The term defines the rate of time taken to reach the sink by overcoming the drawbacks caused due to delays caused due to path discovery, queuing. The parameter can be estimated by dividing the time taken for the packets transmitted to reach the sink from the time at which the packet was transmitted from the origin.

$$\text{Average End – to – End Delivery} = \frac{Timeforpacketfromsource}{Timeforpackettoarriveatdestination}$$

C. End – to – End Delay:

The metric defines the period taken by the data packet to attain the sink after generated from a source. The delay can be calculated by calculating the overall packets reached the sink through traffic after a long term. It also affects the data packets that are queued at the source.

$$\text{End – to – End Delay} = \frac{Ave\arg ePacketsarrivedatthes\text{in}\,k}{Traffi\;\text{cov}erthenetwork}$$

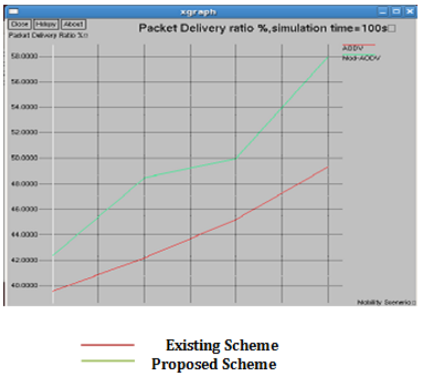


Fig. 3a: Packet Delivery Ratio over time 100s.

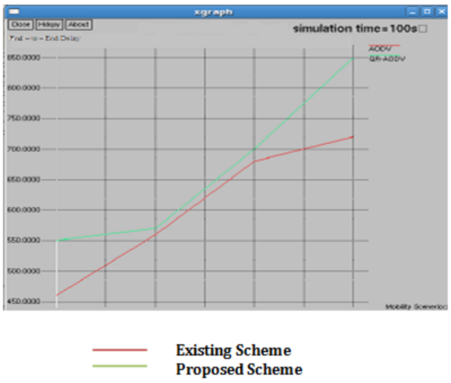


Fig. 3b: Average End – to – End Delivery over time 100s.

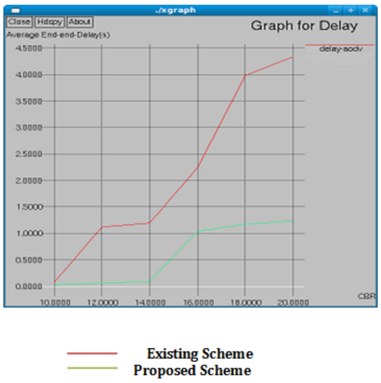


Fig. 3c: Average End – to – End Delay over time 100s.

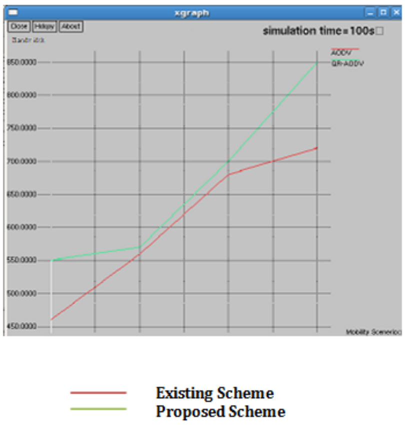


Fig. 3d: Estimation of Bandwidth over time 100s.

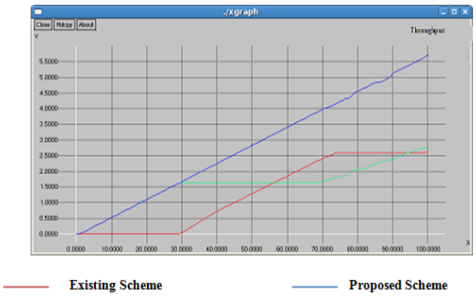


Fig. 3: Estimating the output efficiency over 100s with high network density.

D. Throughput:

The metric defines the packets in total transmitted to the sink over the estimated period of time. The throughputs for the algorithms performance are done for a set of 50, 100 and can include large margins.

$$Throughput = \frac{Numberofpacketsreachingthedestination}{NodePopulation}$$

E. .Estimation of Bandwidth:

The prediction of bandwidth is essential since it permits a node to make most favorable decision in order to transmit the packets through the network before the actual transmission starts. The metric provides a clear idea about the bandwidth available through estimation for enhancing good quality service through the network. It is not an easier task of estimating the bandwidth over the network since they are shared among the neighboring nodes where every other node does not have any prior knowledge about that nodes traffic density. The following graph denotes the ratio between number of packets and messages transmitted successfully. In the existing method the messages transmitted successfully is less than the number of packets due to insecurity. In this proposed method, the messages transmitted successfully are equal due to multi stage monitoring.

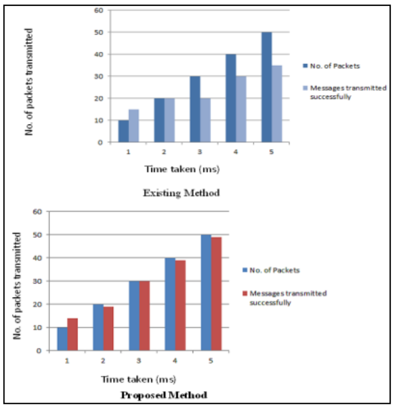


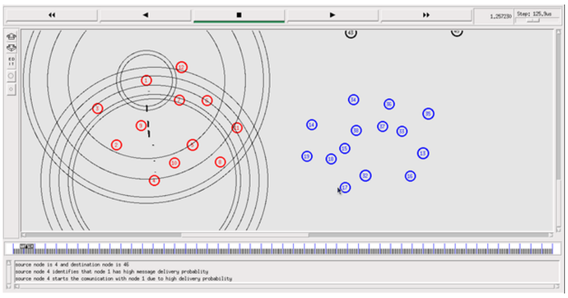
Fig. 4: Comparison of ratio between number of packets and messages transmitted.

Performance Metrics Analysis:

Multi stage security established for node 1 is given in red color and it sends packets to other nodes through a secure link. Unsecure nodes detected using the SCR algorithm are given by interconnected rings. Multi stage security is enhanced inorder to reach the nodes through a secure link. The nodes encircled red color are secure nodes since multi stage monitoring is provided which is shown in the simulation.

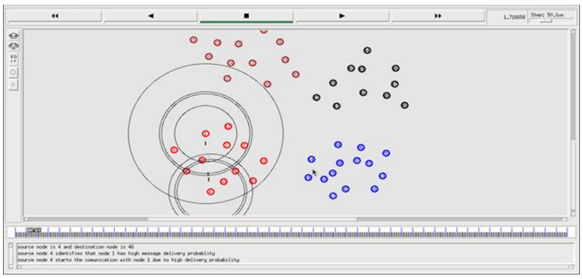
Parameters	Efficiency Percentage	
	Existing Method	Proposed method
No of nodes	50, 100, 150, 200, …	50, 100, 150, 200, …
Packet delivery ratio	63.08	80.13
Average End to end delivery	0.047s	0.044s
End to end delay	0.042s	0.039s
Throughput	250 Packets	300Packets
Bandwidth	1 Mbps	1 Mbps

Resultant Output:



source node is 4 and destination node is 46
source node 4 identifies that node 1 has high message delivery problity
source node 4 starts the comunication with node 1 due to high delivery probability

Fig. 5: Multi stage security is established for node 1 in red colour and sending packets to secure link to other nodes.



```
source node is 4 and destination node is 46
source node 4 identifies that node 1 has high message delivery probablity
source node 4 starts the comunication with node 1 due to high delivery probability
```

Fig. 6: Multistage security increased through a secure link

Figure 6 shows unsecure nodes in the interconnected rings. But multi stage security is increased through a secure link. The encircled red circle shows the secure nodes which will be provided with multi stage security. Further the nodes are linked to provide multi stage security for other nodes.

Conclusion:

This paper presents the architecture, the computation and the implementation of the Security based Context-aware Adaptive Routing protocol which supports communication in delay tolerant mobile ad hoc networks [20]. It shows that conjecture techniques can be used to design backlog and lead mechanisms to transmit messages in intermittently connected mobile ad hoc networks, where a connected path between the sender and receiver may not abide. A generic framework was designed for the evaluation of multiple dimensions of the mobile context in order to select the best message carrier. The paper also demonstrated that Kalman filter based anticipating techniques can be applied effectively to support message forwarding.

REFERENCE

Perkins, C.E., 2001. Ad Hoc Networking. Addison-Wesley.

Fall, K., 2003. ‘Delay-tolerant network architecture for challenged internets’, in Proceedings of SIGCOMM’03.

Vahdat, A., and D. Becker, 2000. ‘Epidemic Routing for Partially Connected Ad Hoc Networks’, Department of Computer Science, Duke University, Tech. Rep. CS-2000-06.

Jain, S., 2004. ‘Routing in a delay tolerant network,” in Proceedings of SIGCOMM’04.

Zhao, V., 2004. ‘A message ferrying approach for data delivery in sparse mobile ad hoc networks’,in Proceedings of MobiHoc’04.

Sarafijanovic-Djukic, M.P.N. and M. Grossglauser, 2006. ‘Island Hopping:Efficient Mobility Assisted Forwarding in Partitioned Networks,’ in Proceedings of IEEE SECON’06.

Lindgren, A., 2003. ‘Probabilistic routing in intermittently connected networks’, Mobile Computing and Communications Review, 7-3.

Spyropoulos, T., 2005. ‘Spray and wait: an efficient routing scheme for intermittently connected mobile networks’, in Proceeding of WDTN’05. New York, NY, USA: ACM Press, 252-259.

Keeney, R.L. and H. Raiffa, 1976. ‘Decisions with Multiple Objectives: Preference and Value Tradeoffs, ser. Wiley Series in Probability and Mathematical Statistics’. John Wiley and Sons.

Musolesi, M., 2005. ‘Adaptive routing for intermittently connected mobile ad hoc networks’, in Proceedings of WoWMoM’05. Taormina, Italy. IEEE press.

Musolesi, M. and C. Mascolo, 2007. ‘Designing mobility models based on social network theory’, ACM SIGMOBILE Mobile Computing and Communications Review, 11[3].

Perkins, C.E. and P. Bhagwat, 1994. ‘Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers’, in Proceedings of SIGCOMM’94.

Taha, H.A., 1996. Operations Research: An Introduction. Prentice Hall.

Kalman, R.E., 1960. ‘A new approach to linear filtering and prediction problems’, Transactions of the ASME Journal of Basic Engineering.

Pasztor, B., 2007. ‘Opportunistic Mobile Sensor Data Collection with SSCR’, in Proceedings of MASS’07. Pisa, Italy: IEEE Press.

Bantz, D.F. 2003. ‘Autonomic personal computing’, IBM Systems Journal, 42[1].

Chatfield, C., 2004. The Analysis of Time Series An Introduction. Chapman and Hall CRC.

Malkin, G., 1999. ‘RFC2453 – RIP Version 2’.

Brockwell, P.J. and R.A. Davis, 1996. Introduction to Time Series and Forecasting. Springer.