ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

MUTUAL AUTHENTICATION USING SHARED SECRET KEY GENERATION

M.Vanitha*,
VIT University, Vellore.
Email: mvanitha@vit.ac.in

Received on 06-08-2016 *Accepted on 27-08-2016*

Abstract

Authentication thwarts unauthorized users from accessing resources from insecure network environments. Secret keys can be generated and shared between two wireless nodes by measuring and encoding radio channel characteristics without ever revealing the secret key to an eavesdropper at a third location. This project addresses bit extraction, i.e., the extraction of secret key bits from noisy radio channel measurements at two nodes such that the two secret keys reliably agree. Problems include non-simultaneous directional measurements, correlated bit streams, and low bit rate of secret key generation. Based on cryptographic techniques, several password authentication schemes have previously been implemented. But the mutual authentication should be needed to authenticate the clients. For that purpose, in this paper a secure remote clients mutual authentication scheme using shared secret key generation and that schemes achieves all security requirements by using the Symmetric key algorithm has been proposed.

Keywords: Cryptography, secret key, symmetric key, authentication

1. Introduction

Nowadays, computer system and network becomes high prone to security threats. The introduction of distributed systems and networks measures to protect data during their transmission is called network security. It involves counter measures to protect computer system from intruders.

1.1 Mutual Authentication:

Mutual authentication is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection. And it is also called as Two-way authentication.

1.2 Shared Secret Key Generation

This project investigates the generation of shared secret keys from the observation and processing of reciprocal radio channel properties. Shared secret keys are necessary for private communication over a open channel. Public key cryptography has been the most common method for the establishment of such keys, but concerns about its limitations has spawned interest in new methods for key sharing. For example, quantum cryptography does not use public keys, butis prohibitively expensive for most applications. Shared secret key generation from radio channel measurements, on the contrary, is very inexpensive and can be done with any standard radio devices which can receive and transmit on the same frequency channel. For envision its application in mobile and portable radio communications systems, such as IEEE 802.11 or 802.15.4, which communicate on time-division duplex (TDD) channels.

Shared secret key generation from channel measurements is an application which benefits from the randomness of the multipath channel. It would not, for example, work in a truly free-space environment (such as deep space radio links). Secret sharing benefits from:

1. **Reciprocity of the wireless radio channel**: The multipath properties of the radio channel (gains, phase shifts, and delays) at any point in time and on any given frequency channel are identical on both directions of the link.
2. **Temporal variations in the radio channel**: Over time, the multipath channel changes due to movement of either end of the link, and any motion of people and objects in the environment near the link. An application may specifically request a user to move or shake her wireless device in order to generate more temporal variation.
3. **Spatial variations**: The properties of the radio channel are unique to the locations of the two endpoints of the link. An eavesdropper at a third location more than a few wavelengths from either endpoint will measure a different, uncorrelated radio channel .Essentially, the radio channel is a time and space-varying filter, that at any point in time has the identical filter response for signals sent from a to b as for signals sent from b to a. Although the radio channel is reciprocal, measurements of the radio channel are not reciprocal. Additive noise contributes to each measurement as it does in any received signal. Also, the transceiver hardware used by the two nodes are not identical and affect the signal in each direction in a different way. Furthermore, measurements in both directions of the link cannot typically be made simultaneously, as addressed in the following concepts.

Finally, interference power is asymmetric. The proposed system is susceptible to denial-of-service by jamming, in the same way that the wireless link is susceptible to jamming. If nodes cannot communicate, then they also cannot measure signal strength and share a-secret key. However, if multiple-access interference is infrequent, and two nodes

can receive many packets from each other, they will have many measurements of signal strength, marginally impacted by interference, with which to encode a secret key. This assumes that an acknowledgement protocol is applied so that two nodes agree on which packets are to be used in the proposed system. It refers to these sources of non-reciprocity collectively as 'noise' because they are the ultimate cause of bit disagreements between the secret keys generated at nodes a and b. Bit extraction, *i.e.*, the extraction of secret key bits from noisy radio channel measurements at two nodes such that the two secret keys reliably agree, is a major statistical signal processing problem in shared secret key generation. As opposed to communications signal processing, it has no interest in obtaining the transmitted data from another device. We refer to this problem as a radio channel signal processing problem since measurements of the radio channel are the signal of interest. It contributes a statistical framework and algorithm for bit extraction which extracts a high bit rate with given reliability and ensures a bit vector with nearly zero correlation. This framework is a significant improvement on the state-of-the-art in the research area. Recent results have both suggested and demonstrated bit extraction from a variety of different radio channel measurement modalities (*e.g.*, time delay, amplitude, phase, and angle) Several works limit the number of bits per measurement to one or zero. Several works have decreased the measurement rate because correlation between measurements leads to correlation between bits in the secret key, which is detrimental to the security of data encoded with that key. Both compromises reduce the generated secret bit rate. In addition, solutions are ad hoc; each measurement modality requires a separate methodology for secret key generation. This work provides a framework for bit extraction using three signal processing methods:

1) **Fractional interpolation**: Introduce different fractional delays at each node to account for the fact that the two directional measurements are not measured simultaneously.

2) **De-correlation transformation**: Produces a measurement vector with uncorrelated components via a Karhunen-Lo`eve transformation of the original channel measurement vector.

3) **Multi-bit adaptive quantization (MAQ)**: Converts real-valued channel measurements into bits adaptively based on the measured value, using communication so that both nodes agree on the quantization scheme. This project use these procedures in order to transform correlated, real-valued radio channel signal measurements at two nodes into uncorrelated binary data which has a high probability of bit agreement. It refers to the combination of the methods as **high rate uncorrelated bit extraction** (HRUBE). As discussed above, there are methods, called information reconciliation methods, to resolve bit disagreements between two nodes without giving away the entire secret key.

These methods do give away some information to an eavesdropper; if enough information can be obtained, an eavesdropper could perform a brute force search to find the secret key. It is best to minimize the number of bit disagreements and to know a priori the probability of bit disagreement so that an information reconciliation method can be designed efficiently. This project provides a theoretical framework to design systems with low probability of bit disagreement. It discuss the work in the area of secret key extraction from radio channel measurements, and position this work in that frame. It provides an adversary model and describe the fractional interpolation method used to correct for non-simultaneous radio channel measurements. It presents the decor relation of the measured radio channel signal, and presents the multi-bit adaptive quantization method. Next sections provide the methodology and analysis of high-rate uncorrelated bit extraction. In Section 7, the HRUBE method is implemented in wireless nodes and the bit disagreement rate is shown and compared to the analytical results. Finally, future work and conclusions are presented.

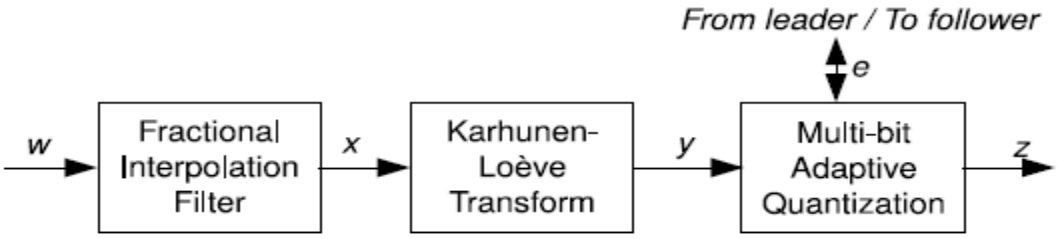


Fig. 1. Flow chart of high rate uncorrelated bit extraction.

2. Problem Statements

This work considers a sensor network in which sensor nodes need to communicate with each other for data processing and routing. It assume that the sensor nodes are distributed to the target area in large numbers and their location within this area is determined randomly. These types of sensor networks are typically deployed in adversarial environments such as military applications where large number of sensors may be dropped from airplanes. In this application, secure communication among sensor nodes requires authentication, privacy and integrity. In order to establish this, there must be a secret key shared between a pair of communicating sensor nodes. Because the network topology is unknown prior to deployment, a key pre-distribution scheme is required where keys are stored into ROMs of sensors before the deployment. The keys stored must be carefully selected so to increase the probability that two neighbouring sensor nodes have at least one key in common. Nodes that do not share a key directly may use a path where each pair of nodes on the path shares a key. The length of this path is called key-path length. Average key-path length, is an important performance metric and design consideration.

2.1 Channel Analysis:

Reciprocity of the wireless radio channel:

The multipath properties of the radio channel (gains, phase shifts, and delays) at any point in time and on any given frequency channel are identical on both directions of the link.

Temporal variations in the radio channel:

Over time, the multipath channel changes due to movement of either end of the link, and any motion of people and objects in the environment near the link. An application may specifically request a user to move or shake her wireless device in order to generate more temporal variation. .

Spatial variations: The properties of the radio channel are unique to the locations of the two endpoints of the link. An eavesdropper at a third location more than a few wavelengths from either endpoint will measure a different, uncorrelated radio channel. Essentially, the radio channel is a time and space-varying filter, that at any point in time has the identical filter response for signals sent from a to b as for signals sent from b to a.

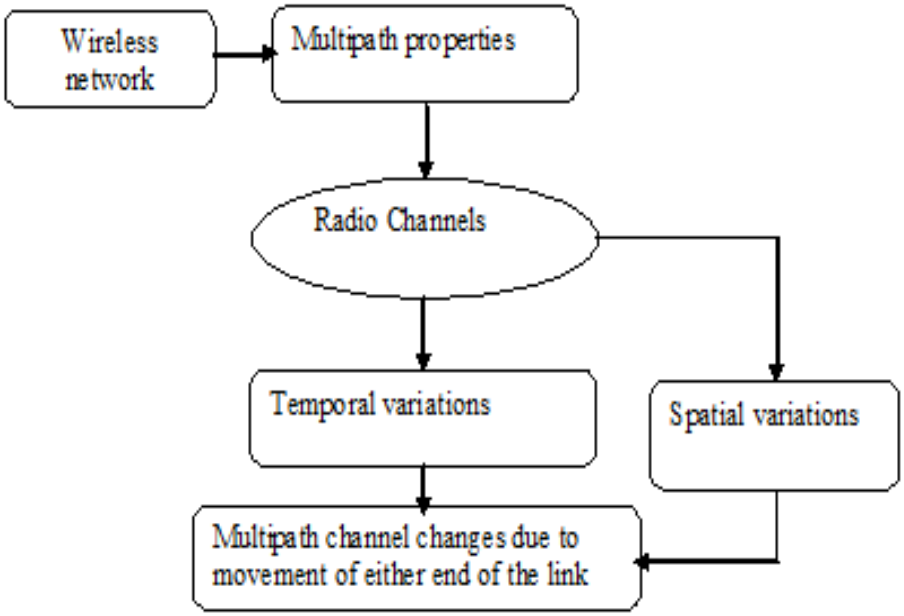


Fig . 2. Channel analysis.

2.2 Decor relation Transformation based KLT Analysis

The discrete Karhunen-Loe`ve transform (KLT) to convert the measured channel vectors xa and xb into uncorrelated components. The KLT has been applied for many different types of signals for purposes of noise reduction and data compression. We apply the KLT for the purpose of generating nearly uncorrelated elements for our secret, which for robustness to attacks, should not contain significant correlation between elements.

The discrete KLT provides an orthogonal basis which decorrelates the input vector, assuming a known model for the covariance structure of the original vector. For particular classes of signals, we can find such statistical models; e.g., for electrocardiogram signals, voice signals, internet traffic measurements, and fingerprints, models have been developed from large sets of measurements. We develop such a covariance model using a large set of measurements, and use it to calculate the appropriate KLT.

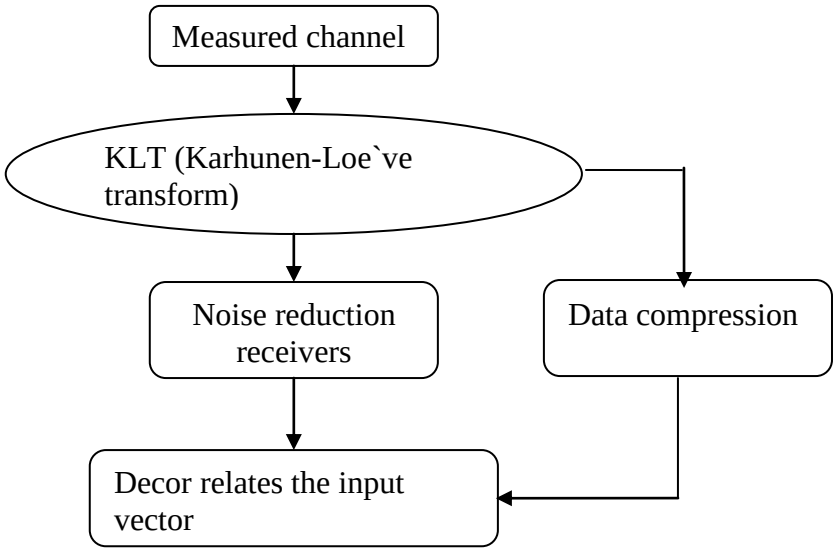


Fig . 3. Decor relation transformation.

2.3 Rijndael Based Key generation:

There have been several papers on the topic of secret key generation from radio channel measurements. In the earliest work, it was suggested to send two unmodulated continuous wave (CW) signals in both directions through a channel and measure and quantize the phase difference between the two at each end of the link to generate a shared secret. Phase differences between multiple channels have been further explored. Time delay and gain are also features of the radio channel that are reciprocal and can be used for secret generation. The impulse response, in particular, the amplitude of multipath at many time delays, can be used as a shared secret. While Madiseh et al. and Wilson et al.use ultra wideband (UWB) radios to measure the impulse response, Ye et al. estimate channel gains and delays from relatively narrowband cellular signals. Amplitude or channel gain is the most common reciprocal channel feature used for secret generation in literature . Amplitude can be more easily measured than time delay or phase on most existing hardware, and thus is more readily applicable to common wireless networks.

2.4 Secret Key Bit extraction:

Bit extraction, i.e., the extraction of secret key bits from noisy radio channel measurements at two nodes such that the two secret keys reliably agree, is a major statistical signal processing problem in shared secret key generation. As

opposed to communications signal processing, it has no interest in obtaining the transmitted data from another device. We refer to this problem as a radio channel signal processing problem since measurements of the radio channel are the signal of interest. This project contributes a statistical framework and algorithm for bit extraction which extracts a high bit rate with given reliability and ensures a bit vector with nearly zero correlation. This framework is a significant improvement on the state of the art in the research area. These methods do give away some information to an eavesdropper; if enough information can be obtained, an eavesdropper could perform a brute-force search to find the secret key. It is best to minimize the number of bit disagreements and to know a priori the probability of bit disagreement so that an information reconciliation method can be designed efficiently.

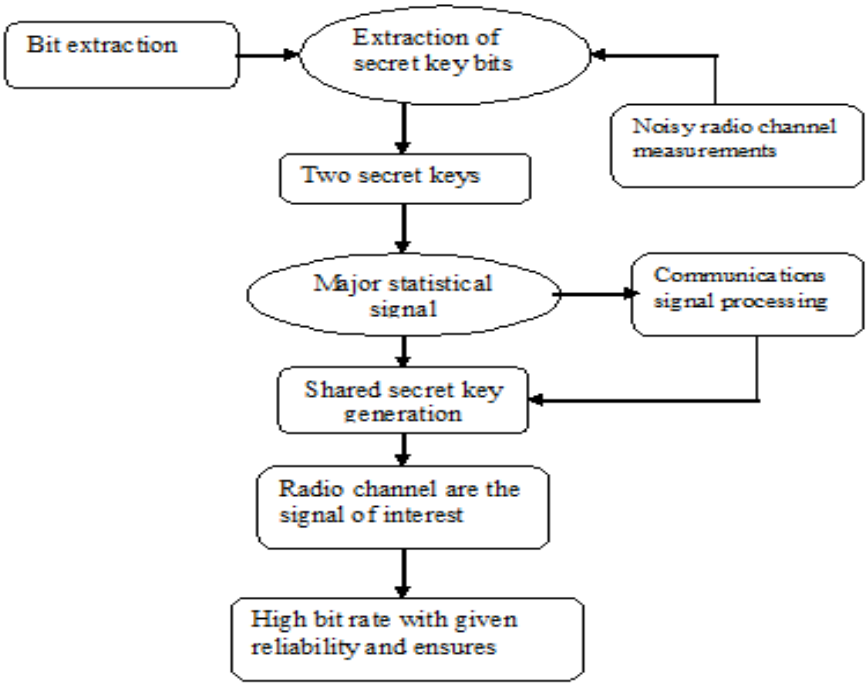


Fig. 4. Secret key bit extraction.

3. Related work

3.1 Maximizing Lifetime of Sensor Surveillance Systems

A sensor surveillance system consists of a set of wireless sensor nodes (sensors for short) and a set of targets to be monitored. The sensors collaborate with each other to watch or monitor the targets and pass the sensed data to the base station. The sensors are powered by batteries and have a stringent power budget. The nature of the sensor surveillance system requires a long lifetime. In this paper, we discuss a maximal lifetime problem in sensor surveillance systems. Given a set of targets, a set of sensors, and a base station (BS) in an area, the sensors are used to watch the targets and collect sensed data to the BS. Each sensor has an initial energy reserve, a fixed surveillance range, and an adjustable transmission range.

A sensor can watch at most one target at a time and a target should be watched by a sensor at any time. The problem is to schedule a subset of sensors to be active at a time to watch the targets and find the routes for the active sensors to send data back to the BS, such that the lifetime of the entire sensor network is maximized. The lifetime is the duration up to the time when there exists one target that can no longer be watched by any sensors or data cannot be forwarded to the BS any longer due to the depletion of energy of the sensor nodes. We assume the positions of targets, sensors, and the BS are given in prior and static. The location information of both sensors and targets can be obtained via a distributed monitoring mechanism or the scanning method by the BS.

The solution to this problem includes two parts: scheduling the sensors to watch targets and routing the sensed data to the BS. The schedule and the routes are pre-computed at the BS, and they are disseminated to sensors by the BS at the system initialization. When the system starts operation, all sensors work according to the schedule, such as when and for what duration to sleep, watch targets, or relay messages. There are many applications of this type of surveillance systems. For example, sensors equipped with camera are used to guard cargo containers to prevent them from being tampered during the long journey of shipment or during the storage at a port. Another example is the use of sensors to monitor some hot spots in a region or in a building. In these examples, sensors and targets are static, and each sensor can only focus on watching one target at a time. For the applications in which one sensor can watch multiple targets simultaneously, some work on sensor scheduling has been done in and, where sensors are scheduled to work in turn such that a given area can be covered fully or partially and the system lifetime is maximized.

3.2 Mobility Improves Coverage of Sensor Networks

The coverage of a sensor network represents the quality of surveillance that the network can provide, for example, how well a region of interest is monitored by sensors, and how effectively a sensor network can detect intruders (targets). It is important to understand how the coverage of a sensor network depends on various network parameters in order to better design and use sensor networks for different application scenarios.

In many applications, sensors are not mobile; they remain stationary after their initial deployment. The coverage of such a stationary sensor network is determined by the initial network configuration. Once the deployment strategy and sensing characteristics of the sensors are known, the network coverage can be computed and remains unchanged over time. Recently, there has been a strong desire to deploy sensors mounted on mobile platforms such as mobile robots. Such mobile sensor networks are extremely valuable in situations where traditional deployment mechanisms fail or are not suitable, for example, a hostile environment where sensors cannot be manually deployed or air-

dropped. Also, in application scenarios such as atmosphere and ocean environment monitoring, sensors move with the surrounding air or ocean currents. The coverage of a mobile sensor network now depends not only on the initial network configurations, but also on the mobility behavior of the sensors.

The coverage of a mobile sensor network from a different perspective. Instead of trying to achieve an improved network configuration as the end result of sensor movement, we identify and characterize the dynamic aspects of network coverage that depend on the movement of sensors. This coverage is not available if the sensors stop moving. We now briefly describe the coverage provided by the sensor movement, and the related research problems.

For mobile intruders, the detection time depends on both the sensor and intruder mobility strategies. We take a game theoretic approach and study the best worst-case performance of a mobile sensor network in terms of the intruder detection time. For a given sensor mobility behavior, we assume that an intruder can choose its mobility strategy so as to maximize its detection time (its lifetime before being detected). On the other hand, sensors choose a mobility strategy that minimizes the maximum detection time resulting from the intruder's mobility strategy. We prove that the optimal sensor mobility strategy is for each sensor to choose its direction uniformly at random. The corresponding intruder mobility strategy is to remain stationary in order to maximize the time before it is detected.

3.3 Detection, Classification and Tracking of Targets in Distributed Sensor Networks

Networks of small, densely distributed wireless sensor nodes are being envisioned and developed for a variety of applications involving monitoring and manipulation of the physical world in a tether less fashion . Typically, each individual node can sense in multiple modalities but has limited communication and computation capabilities. Many challenges must be overcome before the concept of sensor networks becomes a reality. In particular, there are two critical problems underlying successful operation of sensor networks: efficient methods for exchanging information between the nodes, and collaborative signal processing (CSP) between the nodes to gather useful information about the physical world. Energy detection uses minimal a priori information about the target. The detector essentially computes a running average of the signal power over a window of pre-specified length. The output of the detector is sampled at a pre-specified rate. The window duration and sampling rate are determined by target characteristics, such as the signature bandwidth and the expected signature duration in the particular sensing modality. An event is detected when the detector output exceeds a threshold. Due to the inherent signal averaging, the noise component in the output of the detector may be modelled as a Gaussian random variable whose mean and variance can be determined from the statistics of the background noise. The threshold is dynamically adjusted according to the noise

variance of detector output so that the detector maintains a constant false alarm rate (CFAR). If the detector output is below the current threshold, the signal is assumed to consist of noise only and these measurements are used to update the threshold.

3.4 Exposure for Collaborative Detection Using Mobile Sensor Networks

Sensor networks, capable of sensing the environment, exchanging data, processing information, and responding queries, provide an effective connection between computation systems and the physical world. Such networks collect data from the monitored environment and extract useful information to enable a variety of purposes such as battle field surveillance and environmental monitoring. As advances in technology progress, one can envision that mobility will become readily available to nodes for handling more sophisticated sensing tasks in the near future.

In stationary sensor networks, network connectivity and sensing coverage can cause scalability problems in some circumstances. For example, a conventional approach for detecting an intruder in battle field is to deploy a set of stationary nodes in the monitored region. However, if the monitored region is relatively large to either the sensing or the communication range of the nodes, a huge number of nodes are required to be deployed. Typically, the number of nodes to ensure connectivity with a sufficiently high probability in a random deployment is O(L2 log L R2), where L2 is the area of the region and R is the communication range. Similar effect would occur with respect to the sensing range. In such situations, mobile nodes can be an attractive alternative.

4. Implementation

Implementation is the process of converting a new system design into operation. It focuses on user training, site preparation, and file conversion for installing the system under consideration. The important factor that should be considered here is that the conversion should not disrupt the following in the organization.

The objective is to put the tested system into operation while holding costs, risks, and personnel irritation to a minimum.

In my project the conversion involves following steps:

1. Conversion begins with a review of the project plan, the system test documentation, and the implementation plan. The parties involved are the user, the project team, programmers, and operators.
2. The conversion portion of implementation plan are finalized and approved.
3. Files are converted.
4. Parallel processing between the existing and the new systems re initiated.

5. Results of the computer runs and operations for the new system are logged on a special form.
6. Assuming no problems, parallel processing is continued. Implementation details are documented for reference.
7. Conversion is completed at this stage. Plans for the post implementation review are prepared.
8. Following the review, the new system is officially operational.

The prime concern during the conversion process is copying the old files into the new system. Once a particular file is selected, the next step is to specify the data to be converted. A file comparison program is best used for verifying the accuracy of the copying process.

Well-planed test files are important for successful conversion. An audit trail was performed on the system since it is the key to detect errors and fraud in the new system.

During the implementation the user training is most important. In our Web Server project no heavy training is required. Only training how to design and post the files and how to use the administration tools and how to get files etc.

A post-implementation review is an evaluation of a system in terms of the extent to which the system accomplishes stated objectives and actual project cost exceeds initial estimates. It is usually a review of major problems that need converting and those that surfaced during the implementation phase. The team prepares a review plan around the type of evaluation to be done and the time frame for its completion. The plan considers administrative, personnel, and system performance and the changes that are likely to take place through maintenance.

4.1 Cost Estimation of the Project – Cocomo Model

Barry Boehm introduced a hierarchy of software estimation models bearing the name COCOMO, for Constructive Cost Model. The COCOMO models requires seizing information are object points, functions points, and lines of source code.

Object points are sophisticated estimated models (using FP and KLOC) the object point is computed using count of number of screen ,reports and components likely to be required to build the application. Complexity is a function of the number and source of the client and server data tables that are required to generate the screen as report and the number of views.

Once the complexity is determined the number of screens,reports, and components are weighted. The object point count is then determined by multiplying the original instances by weighing factor. Software reuse is to be applied, the percent of reuse is estimated.

NOP= Object Points * [(100-%reuse)/100]

NOP=26 * [(100 – 12) /100]

NOP= 22.88

To derive an estimate of effort based on the computed NOP value,a productivity cost".

PRO=NOP/person-month

PRO=22.88/6

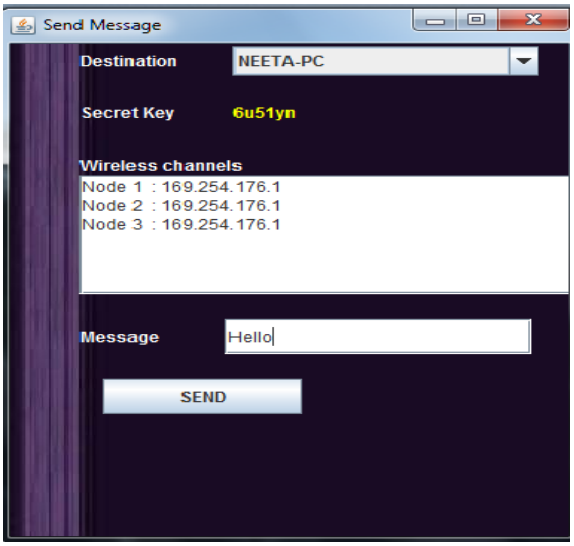
PRO=3.81333

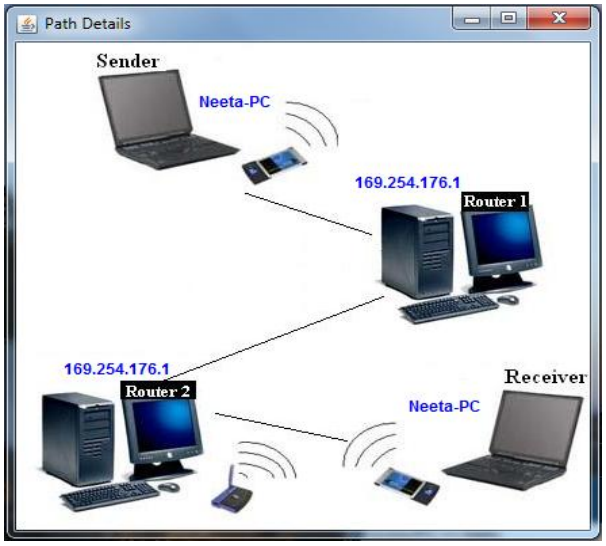
Once the productivity cost has been determined, an estimate of project effort can be derived as,

Estimated effort= NOP/PRO

Estimated effort=22.88 / 3.81333

Estimated effort=6.000052





5. Conclusion

This paperfollows a key pre-distribution scheme, which requires significantly less than $O(n)$ key storage overhead and communication overhead in an wireless ad hoc network with n nodes. The scheme also achieves controllable resilience against node captures. The characteristics of mission-critical networks imply that the proposed scheme is promising in the following aspects.

1. Scalability and the ability to dynamically deploy additional nodes.
2. Resistance against malicious nodes, who pretend to be legitimate nodes (Attack)
3. Resilience to node capture. By our analysis, in order to get better resilience, b cannot be large. Usually b is an integer between 2 to 4.

4. Protection of communication privacy (end-to-end security), such that the talk between any pair of nodes doesn't disclose secret to other nodes.

6. References

1. Patwari, N., Croft, J., Jana, S., &Kasera, S. K. (2010). High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, *9*(1), 17-30.
2. Mohammad,O.K.J., Abbas,S., El-Horbaty,E.-S.M., Salem,A.B.M.(2014).Advanced encryption standard development based quantum key distribution. Proc. IEEE International Conference on Internet Technology and Secured Transactions (ICITST), pp. 402-408.
3. Bat bold Toiruul and KyungOh Lee (2006). An Advanced MutualAuthentication Algorithm Using AES for RFID systems. International Journal of Computer Science and Network Security, vol.6 no.9B,pp.156-162.
4. Bellare, M., &Rogaway, P. (1993). Entity authentication and key distribution. In *Annual International Cryptology Conference*, pp. 232-249.
5. Rice, M. (2009). *Digital communications: a discrete-time approach*. Pearson Education India.
6. Mathur, S., Trappe, W., Mandayam, N., Ye, C., &Reznik, A. (2008). Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking* ,pp. 128-139). ACM.
7. Sayeed, A., &Perrig, A. (2008). Secure wireless communications: Secret keys through multipath. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 3013-3016).
8. Azimi-Sadjadi, B., Kiayias, A., Mercado, A., &Yener, B. (2007, October).Robust key generation from signal envelopes in wireless networks.In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 401-410).ACM.

Corresponding Author:
M.Vanitha*,
Email: mvanitha@vit.ac.in