CHAPTER 6

CONCLUSION

WPAN finds application in control system with safety application like nuclear plants. The issues in WPAN like security, authentication and message integrity and node capture are discussed. Considering these important issues, the research work done in this thesis develops a secured communication protocol for WPAN. To guarantee the security of the algorithm, various encryption algorithms are analyzed. If the encryption algorithm uses ‘n’ bit key then the search space is $2^n$. If the size of the key is large then the search space is also large. A powerful algorithm called Genetic Swarm Optimization which effectively reduces the key search space, is proposed for analyzing the security of cryptographic algorithm.

6.1 ATTACKING KNAPSACK CIPHERS

In this thesis, GSO is first applied to break the knapsack cipher. From the results, GSO performs better than GA and PSO in reducing the search space. The computational complexity in breaking the knapsack cipher is by $O(l)$, where $l$ is the size of the message. The search space and thereby computational time have been reduced by a factor of 6.2, whereas in case of GA and PSO the reduction factor is only 1.6 and 3 respectively. The analysis shows GSO is successful in cryptanalysis. The experimental result indicates that the problem formulation and defining cost function in the cryptanalysis using Computational Intelligence is a tough task. Once the cost function is defined the problem becomes facile.
6.2 ATTACKING S-DES AND DES CIPHERS

Next the block cipher is considered for the analysis. First a simple block cipher S-DES is taken and attacked using Genetic Swarm Optimization. COA is adopted here, which is complex among the attacks. The letter frequency analysis (n-gram statistics) is used as the cost function. It is assumed that the ciphertext is encrypted using plaintext from English language. The letter frequency analysis utilizes up to quadgram statistics and made the research work unique. The analysis says, minimum of 100 ciphertexts are required for the analysis, since the n-gram statistics cannot be computed for less number of characters. This proposed approach can be applied to attack the ciphers constructed using any language other English provided the corresponding language statistics is known. By properly selecting the parameters of GA and PSO, best results are achieved. In case of GSO with hybrid coefficient as ‘1’, the search space have reduced by a factor of 4.3 when compared to Brute-force attack, whereas in case of GSO with hybrid coefficient as ‘0’, the search space have further reduced by a factor 4.8 when compared to Brute-force attack. When hybrid coefficient takes a random value in each iteration, the proposed approach works effectively and reduces the search space by a factor of 5.63 which is a good reduction factor. S-DES is a basal of DES. Hence it is considered first for the analysis. Next 64 bit block cipher is considered for attacking.

In case of attacking DES, KPA is adopted. The correlation function is used a cost function. The performance of GSO is better if the hybrid coefficient lies between 0 and 0.5, than if it lies between 0.5 and 1. From available information, if right pairs of known plaintext-ciphertext pairs are selected then the cost function used is effective and leads to high
successive rate. If the number of known plaintext-ciphertext pairs is more, the cost function is effective thereby increasing the successive rate. The previous research works by Song (2007), Yang (2007) have reduced the rounds in DES and make the problem simple and attacked. In case of Linear and differential cryptanalysis large number of known plaintext pairs are required which is difficult to obtain practically, also these attacks involve in large number of mathematical computation. Only thousand number of known plaintext-ciphertext pairs is considered and the algorithm is run many times to break the key. The proposed approach successfully breaks using a minimum number of known plaintext-ciphertext pairs. This confirms that, the security of DES is not high and can be easily attacked. Hence it is not suitable for the encryption that is to be used for WPAN.

6.3 ATTACKING S-AES AND AES CIPHERS

Next AES is analysed for security. Since S-AES forms the base for AES, it is analysed first and then AES is analysed. KPA and COA are adopted in attacking S-AES. From the analysis, the GSO successfully breaks the S-AES using KPA and COA. In attacking AES, only KPA is used. First GA is applied in breaking the AES and the algorithm could not find the key as the search space is too large ($2^{128}$). The algorithm is tried out for different pairs of plaintext-ciphertext pairs and, GA cannot break the AES cipher. Similarly, attacking the AES is analysed using PSO. Here also it is found that, PSO cannot break the AES cipher. Since the search space is too large, the evolutionary algorithm fails in breaking the AES. This confirms that AES is highly secured and motivated to select the AES algorithm for encryption in the WPAN protocol developed.
6.4 SECURED COMMUNICATION PROTOCOL FOR WPAN

Finally, a highly secured communication protocol is proposed for WPAN. AES algorithm for encryption and MAC is used for message authentication and integrity. Rolling code is used for message freshness which is generated by a NLFSR whose next sequence cannot be predicted. A polynomial based key distribution scheme is also proposed for WPAN, where the node can use single key for each transmission and make the protocol highly secured. Node capture impact is also derived for the polynomial based key distribution. For the proposed scheme NCI is zero, independent of the number of nodes that are captured or compromised. This confirms that the node can be placed even in unsecured environment. Any number of nodes can be introduced in the network without increasing the memory capacity and makes the network highly scalable. This proposed scheme reduces the key access time and consumes limited amount of energy which is the required characteristic for low power sensor nodes. This proposed protocol provides high level of security and is suitable for WPAN.

6.5 SCOPE FOR FUTURE WORK

The future scope of the research work is to analyse the energy requirement for each node and minimise the same. In the sensor nodes the battery has to be replaced at regular intervals. This may be difficult if the nodes are placed in unmanned environment. Hence suitable solution is to use the solar energy so that the energy can be derived by each node using solar cells. The future work is to focus on the utilization of solar energy in WSN.