Non-Cooperative Eavesdropping Resisted Using Ford-Fulkerson And AES By Secure coding

Sreelekshmi Murali
(Dept. of Computer Science and Engineering, Mahatma Gandhi University, Kerala, India)

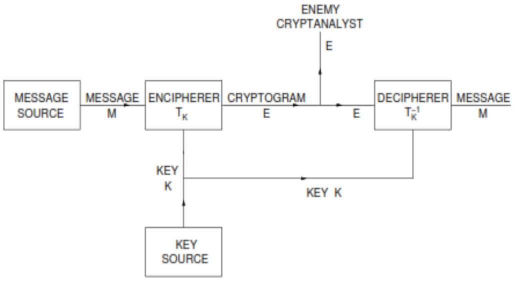
Abstract: *A wireless sensor network is usually composed of a large number of spatially distributed autonomous sensor nodes. Advancement in the field of modern communication networks especially in the wireless network dramatically improved their accessibility,affordability and accuracy. The eavesdropping is a serious security threat to a WSN since this attack is a prerequisite to other attacks. Avoiding the major threat called eavesdropping,cryptographic techniquies are to be used. Reexamine the notion of security,accessibilty,affordability and confidentiality of the WSN, combines Shannon's cypher method and Ford-Fulkerson algorithm together with one time pad system. The idea behind the algorithm is simple. According to Ford-Fulkerson algorithm,as long as there is a path from start node to end node with available capacity on all edges in the path, send flow along one of these paths,find another path and so on.That path is called augmented path. Through this non-cooperative eavesdropping can be avoided. Ford-Fulkerson algorithm can be used along with the one time pad scheme. The one time pad scheme is a binary additive stream cipher, where stream of truly random keys are generated and then combined with the plaintext for encryption or with the ciphertext for decryption using exclusive OR addition. Because of the three important properties of this scheme one time pad scheme can accepted as the most prominent security providing mechanism,properties such as: key must be as long as the plain text, key must be truly random and key must only be used once. Main disadvantage is that one time pad scheme has a serious threat to Brute force attack. Thus for avoiding the brute force attack combines Ford-Fulkerson and ZKP along with the AES algorithm.*

Keywords: *WSN, Non-cooperative eavesdropping,RSA,DES,ZKP,AES.*

I. Introduction

Wireless sensor networks are widely used for various real time applications due to the technological innovations in this domain. The applications of WSN include monitoring wildlife habitat, military and civilian applications where monitoring is essential without human intervention. These applications need complete security as they are vulnerable to various kinds of attacks. However, the nodes in WSN have resource constrined that make them vulnerable for various security attacks. The nodes are wireless with no fixed infrastructure. They work without active operation from human beings. Their energy resources are less and the life time also less for the same reason.. In this paper we focus on the security issues of WSNs. Especially in sensitive applications security plays an important role. The reason behind is that the nodes in WSN are vulnerable to many attacks including node compromizaiton. This is the reason where the security of WSN is significant. Various attacks on sensor nodes in WSN include replay attack, distributed sensor cloning attack and man in the middle attack. With these attacks hackers can gain access to network and obtain sensitive data for monetary gains. In this paper focus on the notion of secrecy system[1] where the adverseries are not subjected to any constraints in terms of their computing power. Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Monitor and eavesdropping also called confidentiality. By listening to the data, the adversary could easily discover the communication contents. Network traffic is also susceptible to monitoring and eavesdropping. This should be no cause for concern given a robust security protocol, but monitoring could lead to attacks similar to those previously described. It could also lead to wormhole or black hole attacks. Eavesdropping is a passive attack that are against the privacy of WSN. With this attack adversaries can listen to the communications over WSN.

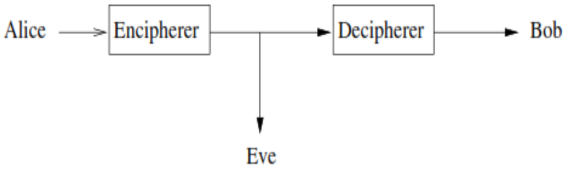
A secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known. ach key and therefore each transformation is assumed to have an a priori probability associated with it—the probability of choosing that key. Similarly each possible message is assumed to have an associated a priori probability, determined by the underlying stochastic process. These probabilities for the various keys and messages are actually the enemy cryptanalyst’s a priori probabilities for the choices in question, and represent his a priori knowledge of the situation. This paper is based on the general secrecy system Fig(1.1) i.e, at the transmitting end there are two information sources- a message source and a key source. The key source produces a particular key from among those which are possible in the system.This key is transmitted by some means, supposedly not interceptible, for example by messenger, to the receiving end. The message source produces a message which is enciphered and the resulting cryptogram sent to the receiving end by a possibly interceptible. At the receiving end the cryptogram and key are combined in the decipherer to recover the message.



Fig(1.1) General Secrecy System

Thus for achiveing the utmost secrecy in WSN, cryptographic algorithms are used. For ensuring this symmetric key and public/private key infrastructures that were developed since 1970s with the advent of computer networks. One of the most important problems in cryptography is the transmission of a secret message between two legitimate users (the sender Alice and the receiver Bob) over an insecure communication channel such that an enemy (Eve) with access to the channel is unable to get useful information about the message being sent. With the goal of solving this problem (or some of its instances), cryptography has provided schemes (ciphers) that “assure security”, in some sense. Almost all the ciphers used are based on the assumption that an enemy has full access to the cryptogram, i.e. the enemy receives an exact copy of the cryptogram, and the goal of these ciphers is to guarantee that there exists no efficient algorithm for breaking, for some reasonable definition of breaking. The problem is that for no existing cipher can this so called “computational security” be proved, without invoking an unproven intractability result. The security of the majority of the most used ciphers is based on the (unproven) difficulty of factoring large integers (for example, the RSA public-key crytosystem) or on the unproven difficulty of computing discrete logarithms in certain groups. Most commonly used cryptograpic algorithms are RSA, DES etc. but these algorithms are not entirely surprising. For cryptography in WSN RSA kinds of algorithms can’t be used as the nodes in the WSN are resource constrained.

On the other hand, information-theoretic (or unconditional) security gives us the strongest definition of security, but it was, in its beginning, impractical. To be more precise, introduced a model of a cryptosystem Fig(1.2). In this model, Eve has perfect access to the insecure channel, i.e. she receives an exact copy of the cryptogram C, where C is obtained by Alice as a function of the plaintext M and a secret key K, shared by Alice and Bob. This paper mainly concens about noncooperative eavesdropping, for avoiding this Shannon’s cipher system used. consider the Shannon cipher system in a setting where the secret key is delivered to the legitimate receiver via a channel with limited capacity. According to Shannon’s definition, a cipher system is perfect if $I(M;C) = 0$i.e. Eve gains no knowledge about $M$by knowing C. Notice that in this definition of a secure cipher system, no assumption about the enemy’s computational power is made, therefore making the information-theoretic security more desirable in cryptography than computational security,



Fig(1.2) Shannon’s model for a secrecy system

he proved that perfect secrecy can be achieved only when the secret key is at least of the size of the plaintext, i.e.

$$H(K) \leq H(M)$$

In the existing system avoiding the eavesdropping combines the shannon’s cipher system and celebrated Ford-Fulkerson along with one time pad scheme. In cryptography, a **one-time pad** (**OTP**) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with random, secret key (or pad).

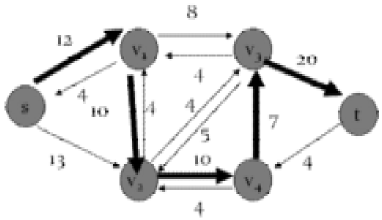
Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, and at least as long as the plaintext, and never reused in whole or in part, and kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. Claude Shannon proved, using information theory considerations, that the one-time pad has a property he termed perfect secrecy; that is, the ciphertext C gives absolutely no additional information about the plaintext. This is because, given a truly random key which is used only once, a ciphertext can be translated into any plaintext of the same length, and all are equally likely. Thus, the a priori probability of a plaintext message M is the same as the a posteriori probability of a plaintext message M given the corresponding ciphertext. Mathematically, this is expressed as H(M)=H(M|C), where H(M) is the entropy of the plaintext and H(M|C) is the conditional entropy of the plaintext given the ciphertext C. Perfect secrecy is a strong notion of cryptanalytic difficulty. Conventional symmetric encryption algorithms use complex patterns of substitution and transpositions. For the best of these currently in use, it is not known whether there can be a cryptanalytic procedure which can reverse (or, usefully, partially reverse) these transformations without knowing the key used during encryption. Asymmetric encryption algorithms depend on mathematical problems that are thought to be difficult to solve, such as integer factorization and discrete logarithms. However there is no proof that these problems are hard, and a mathematical breakthrough could make existing systems vulnerable to attack. Given perfect secrecy, in contrast to conventional symmetric encryption, OTP is immune even to brute-force attacks. Trying all keys simply yields all plaintexts, all equally likely to be the actual plaintext. Even with known plaintext, like part of the message being known, brute-force attacks cannot be used, since an attacker is unable to gain any information about the parts of the key needed to decrypt the rest of the message. Main drawbacks of OTP are:

- it requires perfectly random one-time pads, which is a non-trivial software requirement.
- secure generation and exchange of the one-time pad material, which must be at least as long as the message. (The security of the one-time pad is only as secure as the security of the one-time pad key-exchange). Non information-theoretic-secure ciphers typically only require a cryptographic key, a short string of characters, to be exchanged.
- careful treatment to make sure that it continues to remain secret from any adversary, and is disposed of correctly preventing any reuse in whole or part—hence "one time".

Thus for considering all the drawbacks of OTP, proposed scheme combines Shannon’s cipher system, Zero Knowledge protocol and Ford-Fulkerson algorithm along with AES scheme

II. Related Work

1. *C.E Shannon* [1] proposed a secrecy system. At the transmitting end there are two information sources—a message source and a key source. The key sourceproduces a particular key from among those which are possible in the system. This key is transmitted by some means, supposedly not interceptible, for example by messenger, to the receiving end. The message source produces a message (the “clear”) which is enciphered and the resulting cryptogram sent to the receiving end by a possibly interceptible means, for example radio. At the receiving end the cryptogram and key are combined in the decipherer to recover the message.
2. *N.Cai and R.W. Yeung* [2] proposed a model, call the wiretap network, that incorporates information security with network coding. In this model, a collection of subsets of the channels in the network is given, and a wiretapper is allowed to access any one of these subsets without being able to obtain any information about the message transmitted.Model includes secret sharing in classical cryptography. The main idea in the above scheme is that the sender has to randomize the message in order to protect it from the wiretapper, where in this case the alphabets of the random key and of the information source have the same size. However, model is inefficient and requires a large field size.
3. *J.Feldman, T.Malkin, C.Stein and R.A.Servedio* [3] proposed a network coding model thus provide large field size and model used to achieve min-cut capacity.
4. *Jin Xu and Biao Chen* [4] propsed a combined model of shannon’s cipher system and Ford Fulkerson along with a one time pad scheme. The idea behind the algorithm is simple. As long as there is a path from the source (start node) to the sink (end node), with available capacity on all edges in the path, we send flow along one of these paths. Then we find another path, and so on. A path with available capacity is called an augmenting path as shown in figure



Example for augmenting path (bold edges)

a) No secret key is available *a priori to the source and the sink* nodes. Nonetheless, Shannon's cipher system is inherently useful for such a network setting when there exists route redundancy between the source and the sink nodes.

b) The transmission in each link of the network is subject to non cooperative eavesdropping. Alternatively, there is single adversary, but the link that the adversary chooses to eavesdrop is unknown to the communicating parties.

c) The main contribution of this mechanism is to obtain an achievable rate equivocation region that characterizes the tradeoff between the communication rates and confidentiality.

d) It combines the classical Ford–Fulkerson algorithm for max-flow min-cut network flow and the one-time pad scheme to achieve the desired rate equivocation tradeoff.

e) Existing result is consistent with that of secure network coding when it imposes the perfect secrecy constraint. More importantly, the constructive proof to the achievability constitutes a secure communication scheme that combines the Ford–Fulkerson algorithm and the one-time pad scheme which is both intuitive and easy to implement but yet vulnerable to attacks.

Let $G(V,E)$be a graph, and for each edge from $u$to v, let $c(u,v)$be the capacity and $f(u,v)$be the flow. We want to find the maximum flow from the source $s$to the sink t. After every step in the algorithm the following is maintained, FORD-FULKERSON-METHOD(G,s,t)initialize flow *f* to *0*

while there exists an *augmenting* path *p* do *augment* flow *f* along *p* return *f*

In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.

Main drawbacks of OTP are:

- it requires perfectly random one-time pads, which is a non-trivial software requirement.
- secure generation and exchange of the one-time pad material, which must be at least as long as the message. (The security of the one-time pad is only as secure as the security of the one-time pad key-exchange). Non information-theoretic-secure ciphers typically only require a cryptographic key, a short string of characters, to be exchanged.
- careful treatment to make sure that it continues to remain secret from any adversary, and is disposed of correctly preventing any reuse in whole or part—hence "one time".

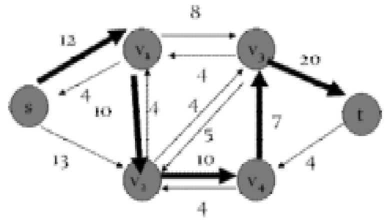
Thus for considering all the drawbacks of OTP, proposed scheme combines Shannon's cipher system, Zero Knowledge protocol and Ford-Fulkerson algorithm along with AES scheme

.

III. Main Result

Proposed scheme combines Shannon's cipher system, Ford-Fulkerson algorithm and Zero Knowledge Protocol along with AES scheme. The Ford–Fulkerson algorithm computes the maximum flow in a flow network. The idea behind the algorithm is very simple: As long as there is a path from the source (start node) to the sink (end node), with available capacity on all edges in the path, we send flow along one of these paths. Then we find another path, and so on. A path with available capacity is called an augmenting path.

The idea behind the algorithm is simple. As long as there is a path from the source (start node) to the sink (end node), with available capacity on all edges in the path, we send flow along one of these paths. Then we find another path, and so on. A path with available capacity is called an augmenting path as shown in figure



Example for augmenting path (bold edges)

a) No secret key is available *a priori to the source and the sink* nodes. Nonetheless, Shannon's cipher system is inherently useful for such a network setting when there exists route redundancy between the source and the sink nodes.
b) The transmission in each link of the network is subject to non cooperative eavesdropping. Alternatively, there is single adversary, but the link that the adversary chooses to eavesdrop is unknown to the communicating parties.
c) The main contribution of this mechanism is to obtain an achievable rate equivocation region that characterizes the tradeoff between the communication rates and confidentiality.
d) It combines the classical Ford–Fulkerson algorithm for max-flow min-cut network flow and the one-time pad scheme to achieve the desired rate equivocation tradeoff.
e) Existing result is consistent with that of secure network coding when it imposes the perfect secrecy constraint.
Let $G(V,E)$ be a graph, and for each edge from u to v, let $c(u,v)$ be the capacity and $f(u,v)$ be the flow. We want to find the maximum flow from the source s to the sink t. After every step in the algorithm the following is maintained: This means that the flow through the network is a *legal flow* after each round in the algorithm. We define the residual network $G_f(V,E_f)$ to be the network with capacity $c_f(u,v) = c(u,v) - f(u,v)$ and no flow. Notice that it can happen that a flow from v to u is allowed in the residual network, though disallowed in the original network: if $f(u,v) > 0$ and $c(v,u) = 0$ then $c_f(v,u) = c(v,u) - f(v,u) = f(u,v) > 0$.Capacity constraints: The flow along an edge can not exceed its capacity. Skew symmetry: The net flow from u to v must be the opposite of the net flow from v to u. Flow conservation: That is, unless u is s or t. The net flow to a node is zero, except for the source, which "produces" flow, and the sink, which "consumes" flow. An augmenting path p is a simple path from s to t on a residual network that is an alternating sequence of vertices and edges of the form $s,e_1,v_1,e_2,v_2,...,e_k,t$ in which no vertex is repeated and no forward edge is saturated and no backward edge is free.
Characteristics of augmenting paths:

- put more flow from s to t through p.
- The edges of residual network are the edges on which residual capacity is positive.
- the maximum capacity by which we can increase the flow on p the residual capacity of p.

Lemma: At each iteration all residual capacities are integers.
Proof: It's true at the beginning. Assume it's true after the first k-1 augmentations, and consider augmentation k along path P. The residual capacity Δ of P is the smallest residual capacity on P, which is integral. After updating, we modify the residual capacities by 0 or Δ, and thus residual capacities stay integers.
Theorem: Ford-Fulkerson's algorithm is finite.
Proof: The capacity of each augmenting path is atleast 1. The augmentation reduces the residual capacity of some edge (s,j) and doesn't increase the residual capacity for some edge (s,i) for any i. So the sum of residual capacities of edges out of s keeps decreasing, and is bounded below 0. Number of augmentations is O(nC) where C is the largest of the capacity in the network.
A flow f is maximum flow in G if :

(1) The residual network G_f contains no more augmented paths.
(2) $| f | = c(S,T)$ for some cut (S,T) (a min-cut).

Proof: Suppose there is an augmenting path in G_f then it implies that the flow f is not maximum, because there is a path through which more data can flow. Thus if flow f is maximum then residual network G_f will have no more augmented paths. Let v=Fx(S,T) be the flow from s to t. By assumption v=CAP(S,T). By Weak duality, the maximum flow is at most CAP(S,T). Thus the flow is maximum.

Zero Knowledge Protocol: This is a protocol which is implemented to ensure security in WSN. This protocol helps the nodes in WSN to have security communications with the need for sharing cryptographic primitives. Thus this protocol plays an important role in WSN in protecting the communications among the nodes and also sinks. The protocol provides an integrative security mechanism those parties such as prover and verifier. The prover can prove the authenticity of a node while the verifier is meant for verifying the authentication of a node. Thus a series of communication takes place in WSN as part of this protocol. The verifier makes challenges and the prover has to replay and prove the genuineness. The computational power consumed by this protocol is also less causing nominal overhead over WSN.

Zero Knowledge protocols allow the prover to prove to the verifier that they know a secret without revealing information about that secret. By comparing values between the commitment and response, the verifier can calculate whether the response matches the expected value. This allows the verifier to verify information without having any knowledge of s, the secret private to the prover.

ZKP must satisfy 3 properties; completeness, soundness, and zero knowledge. The completeness property states that if the statement is true, the honest verifier will be convinced of this fact by an honest prover. The soundness property states that if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability. The zero knowledge property states if the statement is true, no cheating verifier learns anything other than this fact.

ZKP is used to ensure complete security. It can prevent various kinds of attacks such as replay attack, man in the middle attack and also the cloning attack. The ZKP does not let the cryptographic primitives to be moved between the nodes in the netowrk. This is an important feature of the protocol that ensures complete security in WSN.

Proposed scheme can be implemented by combining Fotd-Fulkerson algorithm, Shannon’s cipher system and ZKP along with the AES.

IV. Performance Analysis

The proposed security model is known for its cheaper computational overhead even when compared with public key schemes like RSA. Analysis of Ford-Fulkerson is completely based on analysis of shortest augmenting path. $O(m^2n)$. $O(m+n)$ time to find shortest augmenting path via BFS. $O(m)$ augmentations for paths of length k.

V. Conclusion and Future Work

A wireless sensor network is usually composed of a large number of spatially distributed autonomous sensor nodes. Advancement in the field of modern communication networks especially in the wireless network dramatically improved their accessibility,affordability and accuracy.Wireless sensor network is subjected to several network attacks, among these eavesdropping is the most vulerable attack and is due to the unreliable multihop transmission and intermediate packet mixing. The eavesdropping is a serious security threat to a WSN since this attack is a prerequisite to other attacks. Eavesdropping attacks are especially concerned as they could seriously impair the confidentialty of network coded systems. Avoiding the major threat called eavesdropping,cryptographic techniquies are to be used.But normal cryptograpic algorithms such as RSA and DES fails to avoid the eavesdropping. Reexamine the notion of security,accessibilty,affordability and confidentiality of the WSN, combines Shannon's cypher method and Ford-Fulkerson algorithm together with one time pad system. The idea behind the algorithm is simple. According to Ford-Fulkerson algorithm,as long as there is a path from start node to end node with available capacity on all edges in the path, send flow along one of these paths,find another path and so on.That path is called augmented path. Through this non-cooperative eavesdropping can be avoided. Ford-Fulkerson algorithm can be used along with the one time pad scheme. The one time pad scheme is a binary additive stream cipher, where stream of truly random keys are generated and then combined with the plaintext for encryption or with the ciphertext for decryption using exclusive OR addition. Because of the three important properties of this scheme one time pad scheme can accepted as the most prominent security providing mechanism,properties such as: key must be as long as the plain text, key must be truly random and key must only be used once. Main disadvantage is that one time pad scheme has a serious threat to Brute force attack. Thus for avoiding the brute force attack combines Ford-Fulkerson and ZKP along with the AES algorithm.

References

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst.Tech. J.*, vol. 28, pp. 565–715, Oct. 1949.

[2] N.CaiandR.W.Yeung,“Secure network coding,” presented at the IEEE Int. Symp. Inf. Theory, Jun. 2002.

[3] N. Cai and R. W. Yeung, “Secure network coding on a wiretap network,” *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[4] J.Feldman,T.Malkin,C.Stein,andR.A. Servedio, “On the capacity of secure network coding,” presented at the Allerton Conf. Commun., Control Comput., Sep. 2004.

[5] Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Identity for Ad Hoc Wireless Networks An In-Depth Study, Technical Report, 2003. http://www.cs.rit.edu/ jsb7384/zkp-survey.pdf

[6] L.K.FordandD.K.Fulkerson, *Flows in Networks*. Princeton, NJ, USA: Princeton Univ. Press, 1962.

[7] Jin Xu and Biao Chen,” Secure Coding Over Networks AgainstNoncooperative Eavesdropping” IEEE Transactions On Information Theory, VOL. 59,NO. 7, JULY 2013