International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 6, Nov.-2016, ISSN (Online): 2395-566X

Ant Colony Based Optimized Encryption Scheme for Network-Coded Mobile Ad-Hoc Networks

Garima Boriya, Anubhav Sharma
Department of Computer Science & Engineering
Acropolis Institute of Technology & Research, Bhopal

***Abstract* – In the recent years, the technology of wireless sensor networks has gained a lot of importance. Proposed methodology present a novel routing protocol for multipath energy efficient routing over sensor network that encapsulate advantage of two different predefine method in order to overcome their limitation. Proposed protocol tries to provide supplement support to lower energy node at heavy traffic by higher energy node from lower traffic of network. In this work outlier detection and the Linear Regression approach has been use as a hybrid approach to find the high energy node. This approach helps to enhance the network survival. The simulation results also provide the batter results as compare to previous approach. The technique was tested through simulations for different distributions of nodes. Under all the evaluated scenarios, the technique demonstrates excellent performance as compare to existing one.**

***Keywords* – Wireless Network, Mobile Ad Hoc Network, Encryption, Energy Saving Routing, Ant Colony Algorithm.**

I. INTRODUCTION

The data aggregation, security and energy consumption are most important issues in Wireless Ad-hoc Networks due to limitation of resources. The distribution of huge number of mobile node over sensing area increases the data correctness. Form [1], The mobile nodes deployed on nearby area can sense the same data, which generate lots of data redundancy. When protocols send extra and un-necessary copies of data, then energy and bandwidth will be wasted. When many nodes sense the same area and send same data packet to their neighbor, in this situation there will be waste of resources in sensor node. This problem can be resolve by data aggregation technique, in which include combination of data by many nodes at intermediate nodes and then transmission will be done to the base station. In network, there is another issue that is data redundancy. Data redundancy is referred to duplicate data. Removing redundancy is a biggest challenge in mobile ad-hoc network.To provide security, the nodes must share a secret key only to the authenticated neighbor nodes, so that we can achieve the various security goals like confidentiality, integrity, non-repudiation, authentication, and availability. To provide the required level of security, a MANET security solution also needs to consume minimum amount of energy owing to the MANET operation in wireless communication environment. Recently, there have been lots of works on developing energy efficient and low cost oriented security method in wireless networks.[1]To provide security for MANETs, only symmetric key encryption algorithms are used but they are not efficient. Network coding can reduce energy consumption with scalability, transparency and performance in MANETs.

Data redundancy relates to a duplicate data. The nodes that are in same region, can sense the same data from various nodes in that network region. If all data nodes will send data to the same node or a base station then node energy will decrease rapidly and energy will be wasted. High redundancy leads to higher correctness in final result. Low rate of redundancy is unfavorable. But large redundant data needs more energy to handle redundancy. Elimination of redundancy is biggest challenge in wireless ad-hoc network. To increase fault tolerance, sensor network reliability, data accuracy, network lifetime and network security, data redundancy should be decrease.

When data will forward to another node in network then the duplicate copies of data can be transferred to the destination via multiple paths and it may be possible that, same data can be transferred through other nodes via same path. In this data forwarding, sender node sends data values that it sensed and received data values that sensed from other sensor nodes in network.

In wireless ad-hoc network, each source transmitted data to destination in multiple hops. Due to unreliable nature of network, we cannot assume that all the time, all nodes in network works correctly. Nodes may be degrades or discharge at any time during transmission in network. In wireless ad-hoc network, sensor node can deliver false data in both data forwarding and data aggregation. The monitoring of data by data aggregator conducts data aggregation and generate small-size authentication code message for verification of data. Data integrity verifies by the sensor node between two consecutive aggregators, it can verify integrity on only encrypted data instead of plain data and it can provides secure data transmission.

The presented study addresses the issues of MANET. In such kind of network not a fixed infrastructure available, additionally the main issue arises when the network devices are wondering over the whole network area randomly. So, the topology development and maintenance is responsibility of routing strategy. Therefore, the mobility is a domain of interest that is responsible for frequent path break and re-initialization of route discovery by which the network performance is degraded considerably.

In addition of that, the MANET devices are designed with limited memory, computational and energy resources. Once these resources are consumed, than recovery of energy like resources rapidly during the communication is a complex issue therefore, to maintain the efficiency and power consumption is also a significant issue in this context.

II. PROPOSED METHODOLOGY

Mobility and energy consumption are complex issue in the ad hoc network, due to high and frequent mobility network partitioning like issues are arises. Therefore, that is router's responsibility to arrange the path and save energy in ad hoc network. So, here required to find a search technique, by which efficiently the new path discovered due to path break and/or link failure and consumes less energy. Thus here a clustering technique, i.e., k-means clustering and a cryptographic scheme, i.e., p-coding are used in proposed method, over the conventional routing techniques.

This paper studied the problem of energy saving in MANETs based on the technique of network coding. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. We proposed optimized P-Coding, a lightweight scheme on top of network coding, to further reduce energy consumption in MANETs by cutting the security cost. For optimization proposed technique use ant colony optimization scheme. Optimized P-Coding exploits the intrinsic security property of network coding, and uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. We will showed that optimized P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

III. P-CODING

The P-Coding scheme performs permutation encryption on the coded messages.Permutation encryption scheme, [2] P-coding which is more efficient and assures confidentially. The basic idea of this scheme is permutation encryption is applied on each packet before performing network coding operations. Without knowing the permutation, eavesdroppers cannot decode, and thus cannot obtain any meaningful information.

Let $m = [m1,m2,\ldots\ldots mn]$ be a sequence of symbols and k be a permutation have length n, then PEF (Permutation Encryption Function) on m by key k is defined as:

$Ek(m) = [mk(1), mk(2),\ldots\ldots mk(n)]$

Similarly, Permutation Decryption Function on c by key k as $Dk(c)$,

$Dk(Ek(m)) = m$

Here, k is the PEF key.

Permutation encryption is easy and simple to cryptographic analysis. The main idea of P-coding is to use permutation encryption on coded message. Message symbols and corresponding GEVs (Global Encoding Vector) mixes after PEF operation and it can reordered the message. There is a Key Distribution Centre (KDC) that generates symmetric keys so that sender and receiver can share the PEF key 'k' in P-coding.

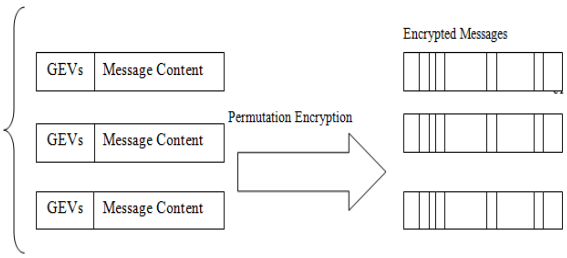

Fig.1. Permutation Encryption on Coded message

In other word, from above fig. 1, in the network each node prefixes the Global Encoding Vector (GEV) to the packet. Permutation encryption operation randomly mixes the symbols of the messages and corresponding GEVs. This operation creates considerable confusions to the eavesdroppers. Generally P-Coding scheme consists of three stages: source encoding, intermediate recoding, and sinks decoding.

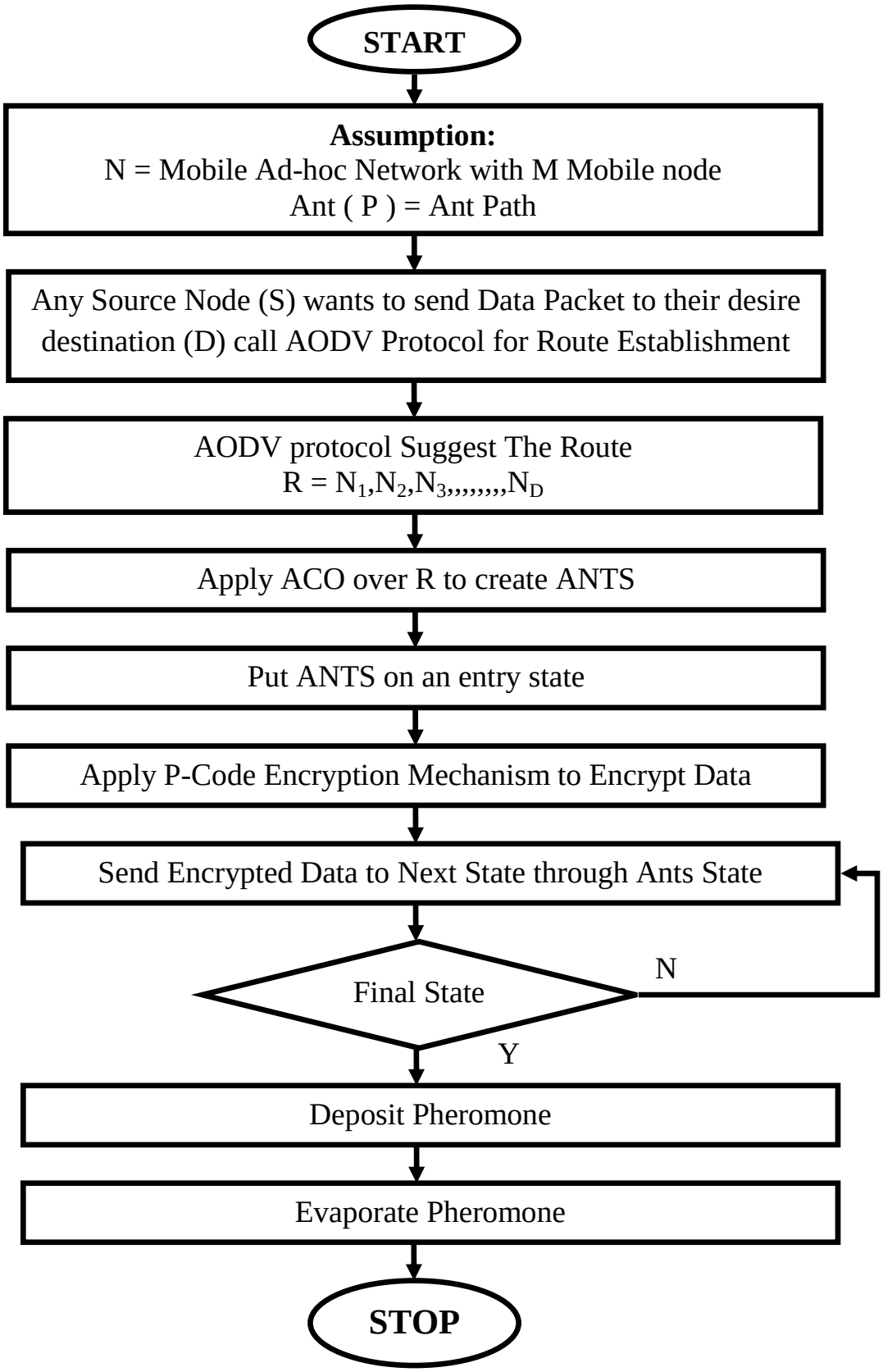

Fig.2. Flowchart of Algorithm Designed

International Journal of Scientific Research & Engineering Trends
Volume 2, Issue 6, Nov.-2016, ISSN (Online): 2395-566X

a. **Source Encoding**

Consider in general that a source s wants to transmit h messages. Each message is prefixed with the GEV and permutation encryption operation is performed. Finally the encrypted message is generated.

b. **Intermediate Recoding**

As the symbols of messages and corresponding GEVs are rearranged by permutation encryption operation it is difficult to construct the source messages. The intermediate nodes have no idea of the key being used and hence it is difficult to decrypt the message.

c. **Sink Decoding**

At the sink node the cipher-text is received and decrypted using the permutation decryption operation. Finally the original message is obtained by applying Gaussian elimination.

IV. Simulation Detail & Result Analysis

Simulation of propose routing protocols is carried over NS-2 to evaluate the performance. Various parameters that are considered for simulation are listed in table 1

Parameters	**Values**	
Number Of Nodes	Vary From 10 To 100	
Area Size	40	600*300
	50	600*300
	100	1000*800
Mac	802.11	
Routing Protocol And Techniques	Aodv, Aco And P-Coding	
Simulation Time	300mili Seconds	
Traffic Source	CBR	
Packet Transmission Rate	1024 Kbps	
Transmit Power	1.0 W	
Receiving Power	1.0 W	
Idle Power	1.0 W	
Initial Energy	1000 Joules	
Transmission Range	200 Meter	

Energy Consumption by Node: Energy consumption means battery power used by any node for successful transmission. Higher energy consumption degrades the survival of network. And lower energy consumption maintains longer survival of network. For any ideal conduction network need longer survival. Using this protocol the retransmission will be reduced where existing methods are only able to minimized redundant path. Existing approach by using P-code Based On have required higher battery power consumption as compare to proposed methodology by using Ant P-code .

Fig.3. Compression of Energy Consumption

Encryption Time: - Encryption Time means Time used by any node for successful Encryption of any packet for transmission. Higher Encryption time degrades performance. And there is need to develop a system required lower encryption time. For any ideal conduction network need fast encryption algorithm. Using this protocol the retransmission will be reduced where existing methods are only able to minimized redundant path. Existing approach by using P-code Based On have required higher encryption time as compare to proposed methodology by using Ant P-code .

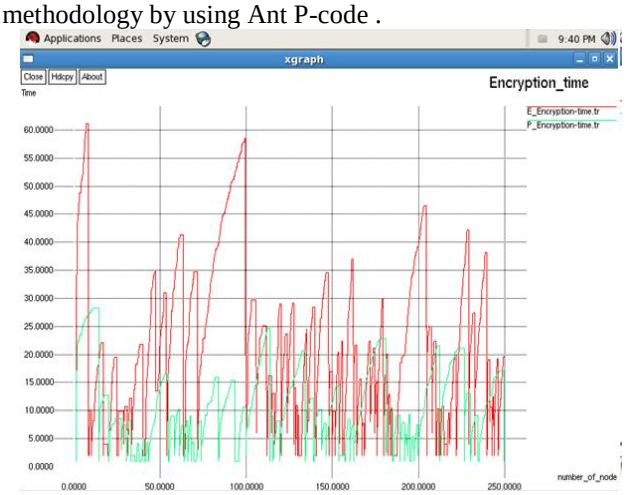

Fig.4. Compression of Encryption Time

Recovery Ratio: - Recovery Ratio means number of time attacker node crack the encryption code. Higher Recovery Ratio degrades performance. And there is need to develop a system required lower Recovery Ratio. Existing approach by using P-code Based On have higher Recovery Ratio as compare to proposed methodology by using Ant P-code .

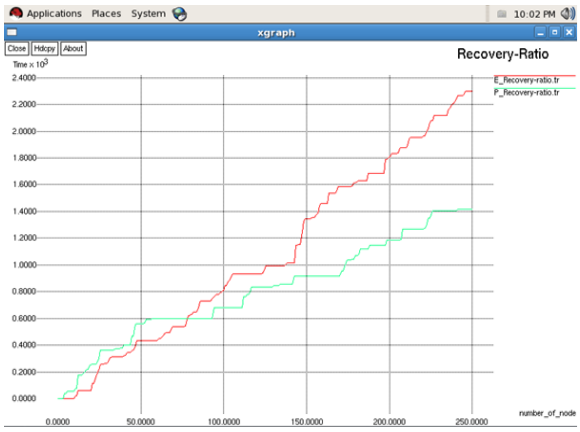

Fig.5. Compression of Recovery Ratio

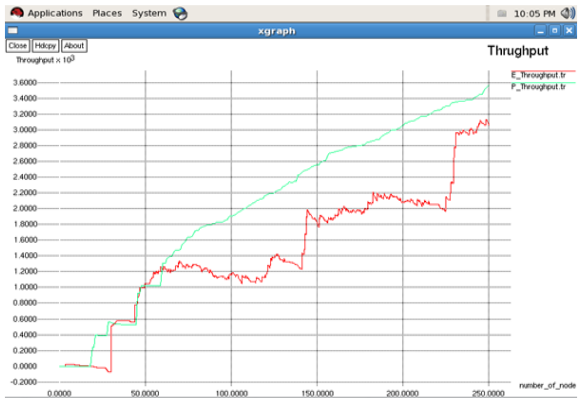

Fig.6. Compression of Throughput

Throughput: -The fraction of the channel capacity for effective transmission (packets successfully delivered to the destination data) is given and is defined as the total number of packets received by the destination. It is in effect a measure of the efficiency of a routing protocol. In any sensor network it is required to have higher throughput ie need to increase rate of successful packet transmission.

CONCLUSION

In the proposed study work described in above section provides the design and implementation of a ACO and P-Coding based routing protocol. To identify the need of protocol we study various techniques by which we get the problem domain and the solution domain. To design the protocol we study the techniques of cryptography and clustering with AODV routing protocol. . But in future their performance can increase by using more suitable clustering algorithms or variation of K-means algorithms. So, in near future we stick with the same concept and we will try to implement this concept with more adaptable clustering algorithm that can reduce more energy.

REFERENCES

[1] Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2010, pp 1-4.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[4] Verma, M.K. and Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.

[5] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[6] Ren Yueqing , Xu Lixin A study on topological characteristics of wireless sensor network based on complex network", IEEE 2010, pp 486 - 489

[7] Bala Krishna, M., Doja, M.N., "Self-organized energy conscious clustering protocol for wireless sensor networks", IEEE 2012,pp 521 - 526

[8] Boniewicz, Miroslaw Toruń, Poland Kozlowska, Anna ; Zawadzka, Anna ; Lukasiak, Zbigniew ; Zielinski, Marek "Review of selected algorithms in the method energy evening algorithm in wireless sensor network", IEEE 2014, pp 1 – 4.

[9] Hartwell, R. , Wireless Sensor Network Energy Use While Tracking Secure Area Intrusions" IEEE 2013, pp 1696 – 1701

[10] Baghyalakshmi, D. ; Ebenezer, J. ; SatyaMurty, S.A.V. "Low latency and energy efficient routing protocols for wireless sensor networks", IEEE 2010, pp 1 – 6.

[11] Peng Zhang, Chuang Lin "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks" in IEEE Transactions on Parallel And Distributed Systems, 1045-9219, 2013 IEEE