International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 29783-29796

http://www.ripublication.com

Secure and Resource Optimization Mechanism for Improvising Privacy and Throughput in Wireless Networks

D V Srihari Babu
Dept. of Electronics and Communication Engg.
Kottam Karunakara Reddy Institute of Technology
Kurnool, India, Srihari2k1@gmail.com
P Chandrasekhar Reddy
Dept. of Electronics and Communication Engg.
JNTUH College of Engg., JNTUH
Hyderabad, India

Abstract

Ensuring privacy and quality of service in wireless communication is a critical issue. It is common that different wireless device coordinates or relies on third party to solve their privacy problems. But at the same time no device wants to share its data for the solution unless a secure privacy is guaranteed. Different privacy based approaches are proposed to provide the privacy but they are lack of proper optimization and quantification in location privacy and resource optimization. This paper contributes a secure policy agreement (SPA) and data privacy mechanism for ensuring privacy. It also presents an energy resource optimization scheme for improvising throughput in wireless communication. SPA implements the secure route discovery mechanism and securing data routing mechanism with energy resource optimization scheme to minimize the energy utilization for achieving high throughput. We evaluate our proposal through simulated experiments with varying different attacker nodes. A performance analysis of throughput, communication overhead, average energy consumption and computation delay is made to evaluate privacy and throughput.

Keywords: Wireless Communication, Secure Policy, Privacy Optimization, Throughput, MANET

Introduction

Wireless networks have been envisioned as a technology that has a great potential to be widely used in various applications. Wireless networks rely on wireless medium of communication, which is by nature a broadcast medium that is more vulnerable to

security attacks due to lack of a physical limitation. Device with wireless receiver can intercept and monitor network communication if adequate security and privacy are not in place. It is become more challenging in case wireless adhoc network as it lack of any support physical infrastructure.

It even more complicated to provide privacy service in wireless network as the sensor nodes are confined to resource limitation in terms of low cost and power [24]. Therefore, high computation cryptography mechanism or public-key cryptosystems are infeasible to wireless communication. This makes it extremely challenging task for researchers to present privacy service in wireless network. Security is largely ignored in traditionally to optimize the sensor node limited capabilities and their applicability to the specific nature. This makes high scopes of security attacks in wireless network [23][25].

In this paper, we propose a secure privacy scheme that provides both privacy routing and resource optimization through secure routes discovery and data routing. In the first phase, a secure policy agreement approach is presented for securing the open-privacy routing in wireless communication using location-centric communication model to achieve efficient security and privacy against both Internal and External adversary pretenders during route discovery process and in second phase, secure data routing through random route key created during the data routing process. For efficient routing and resource optimization we integrate the energy control techniques to minimize energy consumption and high throughput.

The rest of this paper is organized as follows: In Section II, the existing approaches are reviewed in related study. The ptoposed privacy and resource optimization mechanism is described in Section III. In Section IV we presents experiment and performance analysis of the proposed privacy mechanism. In section V we conclude the conclusion and future work.

Related Study

In recent years different levels of privacy and resource optimization schemes [15] are provided for different anonymous routing mechanisms at different costs for adhoc wireless networks. Most of the studies are based on the high computation cryptography mechanism or asymmetric public key cryptography to achieve secrecy and unlink ability of the routing. Public key cryptography is an expensive operation which provides better support to the protection of privacy but it brings significant overhead which makes it infeasible to wireless communication. Similarly energy is a critical resource in wireless network which controls the node lifetime and handles the computation load. In the following sections we discuss the related works in related to privacy and resource in wireless communication.

A. Privacy Routing In Wireless Communication

Kong et al. [5] proposed ANODR scheme that are based on PKC. He is the first to offer the ability to unlink and secret routing in ad hoc networks. It uses single public and private key pairs to reach the secret and separate routing capability messages. Packets incoming and outgoing data is encrypted and decrypted during the route

discovery by the intermediate node to differentiate links by creating a single public and private key. It makes outsiders attackers difficult to identify the data packet routing using this scheme. It is obtained by publicly labeled data packets for communication.

A particular type of public and private key cryptosystem is proposed in MASK [14] to achieve anonymous communication in MANET. It generates pairs of cryptographic keys for the corresponding factors using a trusted third party authority to maintain privacy. It RREQ process is unprotected which makes a passive adversary threat to locate the source node address, and also the destination node identity. An outsider attacker can easily violate the secrecy of the receptor by claiming links to a destination address based on different RREQ packets with the same destination address as explained in [21].

ALARM [1] is based on the anonymous location aided routing scheme that makes use of cryptography in public key infrastructure and the signature of the group to preserve the privacy route. Group signature is an improvised mode of privacy preservation mechanism that provides the functionality to everyone who checks a group signature that is difficult to interpret who is the signer. But ALARM still loses some of the confidentiality of sensitive information related to the network topology data and the node location info.

B. Privacy and Resource Optimizing Approaches

Most previous resource efficient routing protocols in [8][9][10][11][3] do not take care the data privacy before forwarding data they simply assume that wireless links are reliable. It is attracting more and more attentions to use the limited energy more efficiently and guarantee its normal work under unsafely environment. It is a complex problem about the establishment of routing which can resist the attack should have higher energy efficient.

Energy-aware routing protocols for different-power scenarios are aims directly to minimize the total power consumed over the entire transmission path [16][17]. PAMAS [12] is one such least total transmission energy protocol, where transmission power link cost was set and smallest cumulative energy was compute for the smallest path based on the Dijkstra's shortest path algorithm. Formation of large number of hops leads to the nodes that can dynamically adjust their power based on the link distance. In [20] it presented the link cost that includes the receiver power. By using Bellman-Ford modified form of the algorithm resulted in the selection of paths with smaller number of hops than PAMAS.

Secure energy efficient routing protocol (SERP) is described in [18] for wireless sensor networks. It provides robust transmission of authenticated and confidential data from the source sensor with limited energy budget to the base station. SERP three main objectives are considered during design as ensure energy efficient transmission, maximum lifetime of the network and secure transmission. It also designs for Robust and resilient transmission and capable to detect falsely injected which make SERP better performance in the network.

Power-Aware Route Optimization (PARO) algorithm [8][2] is other wireless routing protocols which have been designed to minimize transmission energy cost. It

is designed for scenarios where the nodes can dynamically adjust their transmission power. It attempts to generate a path with a larger number of short distance hops. The intermediary node monitors an ongoing direct communication between two nodes and evaluates the potential for power savings by inserting itself in the forwarding path replacing the direct hop between the two nodes by two smaller hops through itself.

The Lightweight Security Protocol for distributed wireless network (LSec) is described in [13] which use both symmetric and asymmetric security schemes. It is the energy and memory efficient technique that assumes grouping network nodes into clusters. LSec provides the capabilities of authentication, authorization, confidentiality of data, and protection against intrusions and anomalies. We utilized LSec scheme to propose our data privacy as discussed in section-3.2.

Proposed Privacy Mechanism

Secure Policy Agreement (SPA) for Route Discovery

We propose a SPA Protocol [4] which is differ from all previous on demand routing protocols based on the two key important features. Firstly, SPA in communication paradigm is location centric instead of an identify-centric. Therefore, it does not assume any long term node identification or public keys knowledge. Secondly, it does not require any shared secret keys for neither the pre-distributed pair nor any kind of online server for processing. In compare to ALARM [1], it is very different even though it uses group signatures [22] and also location centric, where as ALARM is exposing to entire topology and it is based on a link state protocol.

A. Privacy Model

To design the privacy model of our protocol we extends AODV [6] routing protocol that provides a stable routing mechanism. Due to its on-demand and reactive nature, it does not propagate topology information. Secure privacy agreement (SPA) is designed to authenticate the source and destination addresses. Intermediate nodes ignoring the current location of the source or the actual information of destination nodes and they are also unauthorized. All communications between the source and destination of the route discovery is encrypted and authenticated using the particular specific session secret key. A trusted third party (TTP) acts as the group's manager is trained to learn the locations nodes involved in communication for both the source and destination. The privacy achieved by SPA is not limited to a specific mobility pattern.

Group Signatures described in [20], which are a block to build for anonymous MANET routing protocols, mainly because they satisfy the property of conditional privacy. It can be considered as traditional public and private key and additional features of privacy secured. In the group signature scheme any member can sign a message to a large and dynamic group to produce a group signature. A member who has a copy of a constant length public key can be able to check a group signature. A signature of authentic group involves a certificate valid signature for the group. It is very difficult to calculate and compare two valid group signatures that are generated

by the group, similar or different. To solve such complex special entity Group Manager (GM) is introduced, which can require a Member to provide the identity and open a group signature to identify the actual signature.

B. Functionality of Secure Policy Agreement

SPA function not allows two nodes to share their secret information. The two keys of public key scheme, public key and a private key are used for tuning the secure policy agreement. The secure policy function proceeds when a receiver publishes its public key. This key is used by the sender to encrypt the message to the receiver. When receiving an encrypted message, the receiver uses its private key to decrypt and recover the original message.

SPA utilizes digital signature and public key signature scheme for message securing. It has been found similar in the public key message authentication schemes. Digital signature schemes allow a signer *S* to "*sign*" a message *m* producing a signature $\sigma(m)$. Knowing *pk*, *m* and $\sigma(m)$, any verifier *V* can verify whether the signature is valid or invalid. If *V* learns that $\sigma(m)$ originated from *S* and *m* has not been modified it consider as valid. The signature scheme implements that for every node *n*, each pair of public and secret keys as *(pk, sk)* generate an output by $Gen(1^n)$ and every $m \in \{0,1\}^*$, the methods which performs the verification and signature are - *Verify(pk, m)* and *Sign(sk,m))=1*.

The protocol has three main entities which follow the SPA to do the role as:

- *Group Manager (GM):* As described above that a TTP acts as GM, and it function is to control the group. It monitors the member's node join and leaving. It also verifies the group signatures to authenticate a member node before joining and leaving the group and also discarding the vulnerable nodes.
- *Group Members:* Group members are the nodes which participate in communication and they should authorize with a valid group signature. Every group members owns a unique public and private key for their unique identification, it is used to sign for group authentication. In addition each group member knows the group public key of all other members of the entire group.
- *Outsiders:* Outsiders are the nodes which are outside the group membership. These nodes can pose their public key and group signature to join group.

Member nodes are identified based on the long standing secret identity which is mapped to a group with a unique private key. The relationship and identity of the node to the group is only known to the group manager.

C. SPA Based Route Discovery Mechanism

The operation flow of SPA mechanism is similar to AODV. It allows a source to discover route to a destination and simultaneously discover multiple routes to destination nodes. The privacy mechanism of SPA is described below steps and shown in Figure-1.

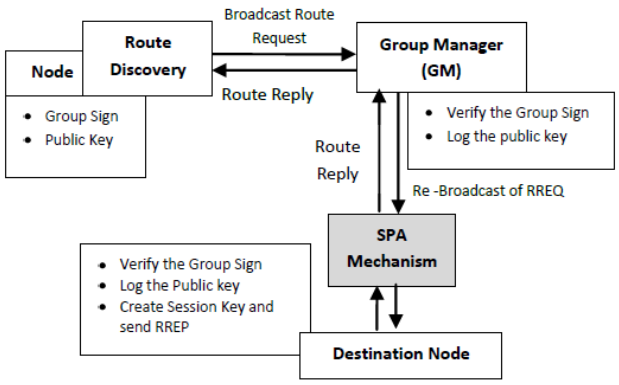

Figure 1: SPA Route Discovery Mechanism

Step-1: The perform route discovery source initiate a route request *(RREQ)*. A *RREQ* contains the address of the destination which to be discover and also consists of source public key as PBK_{SRC_KEY}, group signature as GRS_{SRC_SIG} and packet time stamp as TIS_{SRC_TIM}.

Step-2: The intermediate node on receiving the *RREQ* first verifies the TIS_{SRC_TIM}. In case of invalid, the *RREQ* is dropped, if it is valid then the node verifies whether it is previously processed the similar *RREQ* or not. To validate the previously processed request it generate new hash value of the received *RREQ* and compare with the local hash cache entry, where current *RREQ hashes* are saved.

If the received node is new intermediate node then it caches *Hash (RREQ)* and re-broadcasts the *RREQ* without change of *RREQ* fields. If the node is a destination node then it verifies GRS_{SRC_SIG} and if it found invalid, the *RREQ* is discarded else it save the entire *RREQ* hash value with GRS_{SRC_SIG}.

The destination node on receiving an *RREQ* prepare a route reply (*RREP*) which contains a *Hash (RREQ)*, a new random session key SES_K and an exact destination address location. The obtained *RREQ* are encrypted using PBK_{SRC_KEY}. The *RREP* also consists of the group signature as GRS_{DST_SIG} of all fields and the destination sends *RREP* on the route in which *RREQ* received.

Step-3: Route Nodes on receiving *RREP* verify the cached route *Hash(RREQ)* against the cached *Hash(RREQ)* route. In case of invalid matching it discard the *RREP*. If it is valid then verify for previously not processed the same *RREP*. If it is processed before that it discards the *RREP*, otherwise it updates route table as new active entry and resends the *RREP*. The active route table maintains *Hash(RREQ)* and *Hash(RREP)* for request and reply verification.

Step-4: Source node on receiving the *RREP* from destination, it verifies the correctness of the TIS_{SRC_TIM} and correctness of the location address of the replying node and also verify the group signatures. If *RREP* is found invalid it discards the reply and logged a failure in node log. In case of a valid reply it decrypt the session key and location address using source private key (PVT_{SRC_KEY})provided by the destination The receive key saved by the source and it is used for message encryption and authentication for data message communication.

On completion of the route establishment each source send data message to destination is encrypted with the session key and to maintain the route unique identifier it create a route record of *RREQ* and *RREP* hashes which is in *{Hash(RREQ),Hash(RREP)}* format from source and in reverse it form *{Hash(RREP),Hash(RREQ)}* format from destination.

Data Privacy Mechanism For Data Routing

To maintain the data privacy we create a random route key as R_{key} using Diffie-Hellman algorithm for each route. The route key is created by the destination node on receiving the RREQ message from the source each time, and in reply it sends the route key to source. Source stores R_{key} for each route in route cache table and it will be used during data routing process. To make explicit secure for privacy we will be using this random route key R_{key} during data routing process.

Source node encrypts the data using the random route key as R_{Key} created during the data routing process. Using this mechanism it is capable of maintaining the data privacy during data routing in a route as shown in the equation-2.

$$D_M = Enc_{CA_{pub\_key}}(Enc(Data, R_{key}), D_{add}, T) \quad (2)$$

The data privacy mechanism is described in methods 1 and 2 of the Algorithm-1.

Algorithm 1: Data Privacy Mechanism for Data Routing

Source node *S* init data transmission -> *SendData*(*Data*, D_{add}, *pkt_seq_no*)

Method-1: ***SendData(Data, Destination$_{add}$)***

S gets the shortest route → R_{Path}
S gets Route Key → R_{SKey}

for "number of data packet to send" ***loop***
S creates Data Packet → D_{pkt}
S Encrypt data packet using route key → *Encrypt (Data,* R_{Key} *)* → E_M
S Encrypt data packet E_M → *Encrypt (*E_M, CA_{Pub_key} *)* → D_M
S Sends Encrypted data packet D_M.

while *"ACK_Time expires"* ***do***
.
if "*Receive Message* → D_M" ***then***
S gets Route Key → R_{Key}
S Decrypt the message using CA_{pvt_ey} →
Decrypt(D_M , CA_{pvt_ey} *)* → E_M
S Decrypt the encrypted message using R_{Key} → *Decrypt(*E_M , R_{Key} *)* → *M*

if *M ==*"*DELV_ACK*" ***then***
End while;

Send next data packet → *SendData*(D_{add}, *pkt_seq_no*)
Else if *"ACK_Time expires"* ***then***
Resend the data packet → *SendData*(D_{add}, *pkt_seq_no*)
End if
End while
End for

This method is called on receiving data Packet from Source Node.

Method-2: *RecieveData(D_M, pkt_seq_no)*

Destination node *D* on receiving the data packets,

D gets its own Route Key -> R_{Key}
D Decrypt the message using $CA_{pvt\_ey} \rightarrow$ $Decrypt(D_M, CA_{pvt\_ey}) \rightarrow E_M$
D decrypt the data packets using $R_{Key} \rightarrow Decrypt(E_M, R_{Key}) \rightarrow Data$

D encrypt the *DELV_ACK* message using $R_{Key} \rightarrow Encrypt(DEL\_ACK, R_{Key}) \rightarrow E_M$
D encrypt data packet $E_M \rightarrow Encrypt(E_M, CA_{Pub\_key}) \rightarrow D_M$
D Sends secure acknowledge D_M back to source.

Resource Optimization Mechanism

Traditionally source node sends data to the target node with a path which is used for routing. Multipath routing may improve reliability and reduce energy consumption both as studied in [13]. In this section we discuss our proposed mechanism for how to route optimally between the sources and target node with the minimum expected energy. The least expected energy and reliable unicast routing problem is studied recently in [19]. We extend this approach to find the least expected energy in our proposal for optimal resource manages [7].

The mechanism assigns the power to each wireless node or link to meet the requirement of this routing task. Let assume that $E(x,y)$ represent the assigned power to node x to transmit signal from x to y, and also we assume that each link (x, y) is given an energy resource $E_R(x, y)$ and we compute the energy power E_P required for each link from source *S* and destination *D* such that minimum expected energy for a path connecting S and D will be identified. An energy power E_P will be produce the most energy resource efficient routing for a routing pair of source and target nodes. But it does not mean that it will also produce the most energy efficient routing for all pairs of nodes. However we present a generalized method Algorithm-2 for optimal minimum energy consumption.

***Algorithm-2: Minimum Expected Energy Required for Multipath Routing*.**

Assume that the energy level of source *S* to its *d* neighbor nodes $x_1, x_2, \ldots, x_d$ are $e_1 \leq e_2 \leq \ldots \leq e_d$, where $d \geq k$. Let $E_P = \infty$.

For i=k* till *d loop

Assume source node *S* uses energy e_i.

Node *S* can communicate with all nodes $x_1, x_2, \ldots, x_d$, using energy power e_i.

Let $e_i = \frac{e(s,x_i)}{1-\varepsilon_{s,x_i}(E)}$.

where, $\varepsilon_{s,x_i}(E)$ is the link errors probability.

Assume the cost of each link (s, x_i), for $1 \leq j \leq i$, is *0*.

The each other link cost of link (x, y) is $\frac{E(x,y)}{1-\varepsilon_{x,y}(E)}$.

Find *k* neighbor-node different paths P_i from *S* to *D* with the minimum total link costs δ_i.

If $\delta_i + e_i < E$, then $E = \delta_i + e_i$, and the current best k-neighbor-node different paths *P* is P_i.

End for

Source node *S* transmits at power *E* and the optimum *k*-different path is *P*.

Thus, power level of the source node *S* we fix as *E*, then the problem of finding *k* node different routes with least expected energy link consumption when we set the cost of each link (s,y_i) as 0 for link (s, x_i), with $E(s, x_i) \leq E$. By checking all possible energy levels from the source node to all possible paths, we find the optimum *k*-node different paths for routing.

Experimental Evaluation

Simulation Setup

Simulations are performed using GloMoSim Simulator. It provides simulation statistical data to calculate the performance measurement of the proposed mechanism. The simulation is performed in an area of 1200m x 1200m for 1000sec with varying attacking nodes placed in a random model.

Table 1: Simulation Parameters.

Parameters	**Values**
Simulation Area	1200m X 1200m
Simulation Time	1000 sec
No. of Nodes	50
Pause Time	60 sec
Source-Destination Pairs	20
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility Model	RWP

Mobility Speed	20m/s
Attacker Percentage (%)	0, 10,20,30,40,50

Attackers are randomly selected among nodes during simulation. The attackers drop data packets, but participate in the discovery mechanism correctly. The attack has effect only when attackers are selected in the intermediate nodes of the current data routing path. We use this scenario to evaluate the privacy performance and throughput.

Performance Evaluation

To evaluate the proposed mechanism we compare with a location based link state protocolsuch as ALARM [1] which handles only anonymous location centric MANET routing protocol and a secure and energy efficient protocol as SERP [18] and two energy aware routing protocol as PAMAS [12] and PARO [8] to evaluates the privacy and energy resource consumption performance in different attacker percentage variations. We measure the throughput, communication overhead, average energy consumption and delay analysis to present the performance.

A. Throughput Analysis

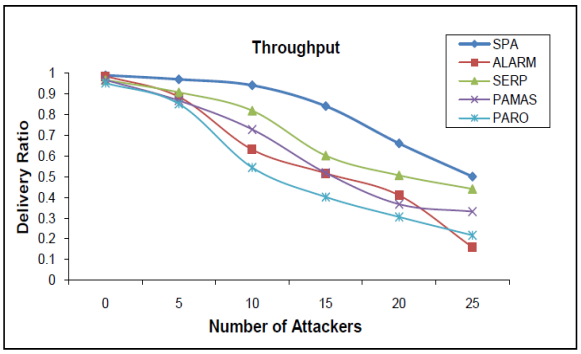

Figure 2: Throughput Comparison

Figure-2 shows the throughput performances of the protocol. All protocol show downfall of the result in case of increased of number of attackers. SPA mechanism shows an improvisation in compare to others protocols schemes. The improvisations of throughput is due to the efficient privacy and resource optimization mechanism which leads to reliable and securing links for data routing and make network lifetime longer which achieve better throughput.

B. Communication Overhead

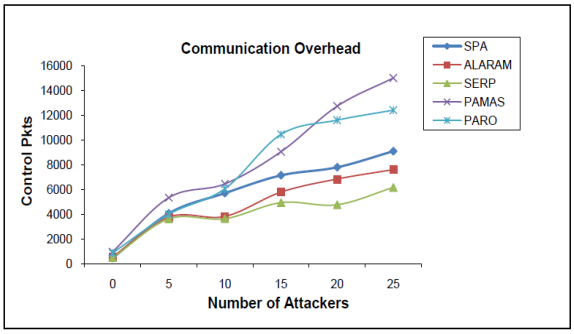

Figure 3: Communication Overhead Comparison

Figure-3 describes the communication overhead between SPA mechanisms with other protocol. It was observed that SPA had reasonable overhead when compared to others. All the protocols show increases in overhead with increment of number of attacks in the networks. The increase of overhead in SPA is due to the introduction of privacy and resource optimization mechanism which increases the number of control packets between the nodes.

C. Average Energy Consumption

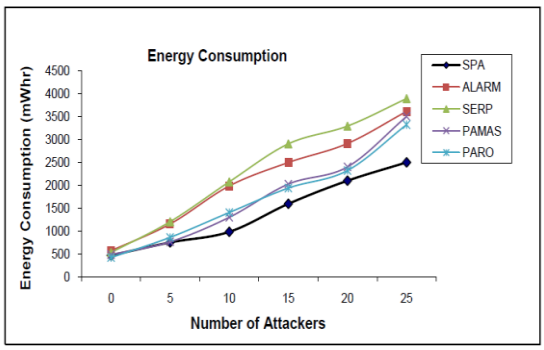

Figure 4: Energy Resource Consumption Comparison

Figure-4 shows the average energy comparison between SPA with others protocols. The increase of number of attackers shows an increase of energy consumption in all the protocols. All protocols shows an steady increment in energy consumption due to high computation requirement with increasing attackers in the network. The protocols which are capable for estimating the energy requirement shows low in compare to other as it minimize the link failure which gives maximum link life time and less power consumption and high throughput.

D. Delay Analysis

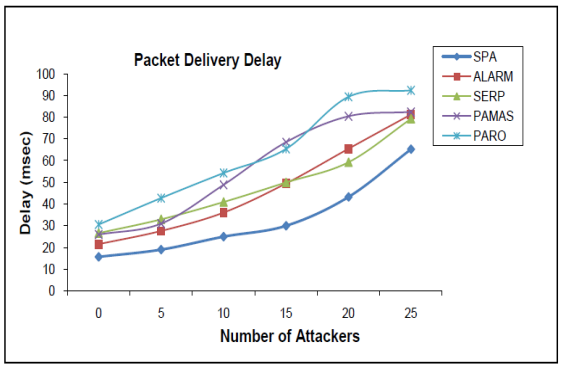

Figure 5: Packet Delivery Delay Comparison

Figure-5 shows packet delivery delay comparison between SPA and others protocols. All the protocols shows similar ratio of increase in delay with increase of attackers. But SPA mechanism shows low delay in compare to other protocols. SPA mechanism follow the process of privacy which allow secure routing and data security in network, which helps in minimizing packet drop and packet delivery delay.

Conclusion and Future Work

This paper presents a Secure Policy Agreement for privacy mechanism with energy resource optimization, which supports the reactive routing environment in suspicious location-based MANET. In literature many energy efficient routing and power assignment protocols have been proposed. However, none of these protocols studies the integration of privacy and energy efficient routing. In this paper we proposed a privacy mechanism for routing and data security with efficient resource management for improvising privacy and throughput. All previous proposed schemes or protocol are efficiently save energy by finding optimal power estimation and shortest route. But these schemes does not take care the data privacy level required for managing link failure due to any attacks. Our proposed approach metric shows a significant drop of energy resource consumption and also a significant improvement over previous method compared due to effective management of resource and privacy. There are many challenges which are left for the future study, such as uniform resource optimization for all nodes for fair routing and impacts of different type of attack to cater the data privacy.

Reference

[1]. K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345-1358, 2011.

[2]. M. Min, F. Wang, D.-Z. Du, and P.M. Pardalos, "A Reliable Virtual Backbone Scheme in Mobile Ad-Hoc Networks," Proc. IEEE Mobile Ad-Hoc and Sensor Systems (MASS), 2004.

[3]. P.J. Wan, G. Calinescu, X.-Y. Li, and O. Frieder, "Minimum- Energy Broadcast Routing in Static Ad Hoc Wireless Networks," Prof. IEEE INFOCOM, 2001.

[4]. D V Srihari Babu, P Chandrasekhar Reddy, "Secure Policy Agreement for Privacy Routing in Wireless Communication System", IEEE, International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),978-1-4799-4190-2/14, 2014

[5]. J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC',pp. 291-302,2003.

[6]. A. Nasipuri, R. Castaneda, and S.R. Das, "Performance of Multipath Routing for On-Demand Protocols in Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications J., vol. 6, no. 4, pp. 339-349, 2001.

[7]. D V Srihari Babu, P Chandrasekhar Reddy, "Privacy and Resource Optimizing Approach for Wireless Ad Hoc Network", ELSEVIER, Proceddings of the Second International Conference on "Emerging Research in Computing, Information, Communication and Applications", ERCICA, 2014

[8]. R. Kravets and P. Krishnan, "Power Management Techniques for Mobile Communication," Proc. ACM MobiCom, 1998.

[9]. V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," Proc. IEEE Int'l Conf. Comm. (ICC), 1998.

[10]. J.-H. Chang and L. Tassiulas, "Energy Conserving Routing in Wireless Ad-Hoc Networks," Proc. IEEE INFOCOM, 2000.

[11]. A. Srinivas and E. Modiano, "Minimum Energy Disjoint Path Routing in Wireless Ad-Hoc Networks," Proc. MobiCom, 2003.

[12]. S. Singh and C. S. Raghavendra. Pamas: Power aware multi-access protocol with signalling for ad hoc networks. ACM Computer Communication Review, 28(3):5.26, July 1998.

[13]. Shaikh, S. Lee, M. A. U. Khan, and Y. J. Song, "LSec: lightweight security protocol for distributed wireless sensor net- work", Lecture Notes in Computer Science, vol. 4217, 2006.

[14]. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in IEEE INFOCOM.,2005

[15]. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks,", pp. 62-68,2001.

[16]. Bin Li, Hongxiang Li, WenjieWang,Qinye Yin, and Hui Liu, "Performance Analysis and Optimization for Energy-Efficient Cooperative Transmission in Random Wireless Sensor Network", IEEE Transactions On Wireless Communications, Vol. 12, No. 9, September 2013

[17]. Chia-Hao Yu, Klaus Doppler, C´assio B. Ribeiro, and Olav Tirkkonen, "Resource Sharing Optimization for Device-to-Device Communication Underlaying Cellular Networks", IEEE Transactions On Wireless Communications, Vol. 10, No. 8, August 2011

[18]. A. K. Pathan and C. S. Hong, "SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network", Annales des Telecomm., pp. 529-541, 2008.

[19]. M. Ahmad, M. Habib, and J. Muhammad, "Analysis of security protocols for Wireless Sensor Networks", in Proc. 3rd Int. Conf. Comp. Res. Develop. ICCRD 2011, Shanghai, China, 2011, vol. 2, pp. 383-387.

[20]. K. Lin, Ch. F. Lai, X. Liu, and X. Guan, "Energy efficiency routing with node compromised resistance in wireless sensor networks", Mob. Netw. Appl., vol. 17, pp. 75-89, 2012.

[21]. A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[22]. S. Canard and M. Girault, "Implementing group signature schemes with smart cards," in CARDIS'02: Proc. 5th conference on Smart Card Research and Advanced Application Conference. Berkeley,CA,USA: USENIX Association,pp. 1-1, 2002.

[23]. E. Kumari and A. Kannammal, "Privacy and security on anonymous routing protocols in manet," in Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on, vol. 2, 28-30 2009, pp. 431-435.

[24]. G. Jakllari, S. Eidenbenz, N. Hengartner, S.V. Krishnamurthy, and M. Faloutsos, "Revisiting Minimum Cost Reliable Routing in Wireless Mesh Networks," Proc. ACM MobiCom, 2007.

[25]. J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in Proc. IEEE MASS', pp. 332-341, 2009.