Protection Profile-Based Scenario-Centric Taxonomy of Secure Routing Protocols in Ad hoc Networks

Mohammad Iftekhar Husain and Ramalingam Sridhar

***Abstract*—Secure routing bears significant importance in wireless ad hoc networks where nodes act both as terminals as well as routers. Although a large body of research exists in literature to address this issue, the variations among the approaches are overwhelming. This necessitates a well-defined taxonomy of existing routing protocols. Current taxonomic approaches for secure routing in ad hoc networks typically do not account for varying security goals and environmental characteristics of different forms of application scenario. In this paper, we present a scenario-centric taxonomy of secure routing protocols in ad hoc networks. We devise a novel framework to define a protection profile for application scenarios that incorporates the notion of security goals, possible attacks and environmental characteristics simultaneously. Finally, we classify the existing secure routing protocols according to their suitability in application scenarios with varying protection profiles. Comparison with existing taxonomic approach shows the effectiveness of our method in terms of completeness, usability and extendibility.**

***Index Terms*—Ad hoc networks, Routing protocols, Security, Classification.**

I. Introduction

An ad hoc network consists of a set of nodes that carry out basic networking functions like packet forwarding and routing without the help of an existing infrastructure or centralized administration. Nodes in an ad hoc network rely on one another for forwarding a packet to its destination, primarily due to the limited range of each host's wireless transmissions. Such interdependency of communication among nodes makes routing in ad hoc networks more vulnerable compared to wired networks.

Several protocols have been proposed in the literature to secure the routing operation in ad hoc networks. Some of the protocols are proposed to address particular attacks. For example, Watchdog and Pathrater [1] are proposed to address routing misbehavior. Some of them just act as a security extension to existing routing protocols such as Secure Ad hoc On-Demand Distance Vector routing [2]. There are also variations in techniques used to achieve security goals as well. For example, message integrity can be ensured by hash or message digest. These factors give an impression that the problem space is vast and hard to explore and address. So, a necessity to classify secure routing protocols arises from the following reasons:

- To choose a protocol appropriate for an application scenario,
- To understand the similarities and differences among protocols,
- To be able to assess the feasibility, effectiveness and cost of deployment, and
- To compare different protocols to each other.

Existing secure routing protocols for ad hoc networks can be classified based on different symmetric, asymmetric and hybrid cryptographic security mechanisms employed to provide security services such as authentication and user integrity. Most often such efforts [3], [4] are based on security mechanisms tailored for specific routing protocols and cannot be used interchangeably with other routing protocols. Secure routing protocols are also classified based on a range of security threats in ad hoc networks. For instance, security protocols such as CONFIDANT [5] are specifically designed to address routing attacks and misbehaviors. However, none of the existing solutions focus on classifying the secure routing protocols according to the intended application scenario of an ad hoc network. The rationale behind such classification criterion is the fact that different forms of ad hoc networks have different security goals and environmental factors.

In this paper, we propose a protection profile based scenario-centric taxonomy of secure routing protocols in ad hoc networks inspired by the notions of the *Common Criteria* [6], the federal criteria for information technology security evaluation proposed by National Security Agency (NSA). We present a framework to define the protection profile for different forms of ad hoc networks. Based on the protection profile, we then analyze the suitability of existing routing protocols for these scenarios. We also compare our taxonomic approach with existing ones in terms of completeness, usability and extendibility.

II. Secure Routing Protocols

In this section, we briefly discuss some representative secure routing protocols proposed in the domain of ad hoc networks.

Authenticated Routing for Ad hoc Networks (ARAN) [7] is a stand-alone secure routing protocol for ad hoc networks. It uses cryptographic certificates to provide authentication and non-repudiation. So, it requires the existence of a trusted Certificate Authority (CA). Each node, before attempting to

M. I. Husain is a PhD student of Computer Science and Engineering, University at Buffalo, The State University of New York, Buffalo, NY 14260, USA (e-mail: imhusain@buffalo.edu).

R. Sridhar is an Associate Professor of Computer Science and Engineering, University at Buffalo, The State University of New York, Buffalo, NY 14260, USA (phone: 716-645-3186; fax: 716-645-3464; e-mail: rsridhar@buffalo.edu).

connect to the ad hoc network, must contact the CA and request a certificate for its address and public key. The protocol assumes that the public key of the CA is pre-distributed among the nodes. Routing traffic messages, such as route discoveries and route replies, must be signed by the node that generates or forwards them. It follows an on-demand approach for basic routing operations.

Secure Efficient Ad hoc Distance vector routing (SEAD) [8] follows a Destination-Sequenced Distance-Vector (DSDV) [9] approach for routing. In order to find the shortest path between two nodes, the distance vector routing protocols utilize a distributed version of the Bellman-Ford algorithm. It uses hash chains to authenticate hop counts and sequence numbers. Generally, a hash chain is created by applying a one-way hash function to a random value repeatedly. SEAD uses the elements of this hash chain to secure the routing traffic. This protocol requires the existence of an authentication and key distribution scheme for security operations.

Ariadne [10] is based on Dynamic Source Routing (DSR) [11] and came from the same researchers who proposed the SEAD protocol. It assumes the existence of a shared secret key between two nodes. Ariadne also uses a message authentication code (MAC) in order to authenticate point-to-point messages between these nodes. TESLA broadcast authentication method [12] is used to authenticate broadcast messages related to routing. The usage of TESLA mandates the presence of strict time synchronization as well.

Secure Link State routing Protocol (SLSP) [13] is a protocol that can be deployed as stand-alone solution for proactive link-state routing, or combined with a reactive ad hoc routing protocol to be used in a hybrid framework. SLSP uses an asymmetric key pair for every a node by which it secures the discovery and the distribution of link state information. Participating nodes are identified by the IP addresses of their interfaces. However, key management and routing misbehavior are not addressed by the authors.

Secure Ad hoc On-Demand Distance Vector routing (SAODV) [2] is a combination of security extensions to the standard Ad hoc On-Demand Distance Vector (AODV) [14] protocol. It utilizes cryptographic signatures to authenticate the non-mutable fields of the messages. The route discovery process is secured using a one-way hash chain. SAODV also assumes the existence of a key management scheme.

Secure Position Aided Ad hoc Routing (SPAAR) [15] uses geographic information and asymmetric cryptography to provide routing security. Geographic information is also used to make forwarding decisions, which reduces routing traffic significantly. Although computation intensive, SPAAR meets most of the security requirements of a scenario.

The CONFIDANT [5] system consists of a set of extensions to DSR that is comprised of a monitor, a reputation system, a path manager and a trust manager. Routing paths are chosen based on the reputation of the nodes which is calculated by monitoring the behavior of that node.

The Watchdog and Pathrater [1] scheme consists of two extensions to the DSR routing protocol. Watchdog is responsible for monitoring the next node in the path whether it forwards the packet properly. Nodes who fail to do so are identified as misbehaving node by watchdog. The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. However, insider attack is not considered in this approach.

Packet Leashes [16] are security extensions that can be used with an existing routing protocol to protect against wormhole attacks. It requires strict time synchronization, or a combination of loose time synchronization and the knowledge of geographical location through GPS.

A. Limitations of Current Secure Routing Protocols

Although a number of secure routing protocols have been proposed in the current literature, these solutions have severe limitations when applied to ad hoc network scenarios with varying topologies. Most of these protocols are developed to target a specific threat or a pre-defined network domain. In ad hoc networks, due to the network dynamics, there is a need to develop and adapt routing protocols according to the demands of the risk and threat level and available resources. Below, we detail some of the factors that limit the applicability of current secure routing solutions to ad hoc networks.

Attack-based protocols: Most of the existing secure routing protocols are aimed at providing solutions to specific types of attacks. For instance, the SAR protocol solves eavesdropping and routing table attacks, but not for other attacks on routing protocols. On the other hand, Ariadne, does not offer any protection against eavesdropping attack. Current solutions are not often equipped to protect against all possible routing threats. This is particularly challenging since ad hoc networks are susceptible to constantly changing attacks and with intelligent adversaries introducing novel attacks.

Key distribution mechanism: Some secure routing protocols such as SAR and SPAAR are based on cryptographic security primitives. However, most of these protocols do not outline or discuss methods for key distribution. As key distribution and management is challenging in ad hoc networks without the presence of any centralized control, we cannot realistically assume the availability of cryptographic keys as proposed in these solutions.

Network environments: Security protocols are mostly developed specific to a network environment. Several assumptions are often made regarding centralized control, trusted entities and available network resources with no clear perspective of the deployment scenario. For instance, the ARAN protocol requires the existence of a trusted CA to authenticate ad hoc routing traffic. Since current protocols do not account for varying characteristics of ad hoc network applications, they do not provide a stand-alone security solution for all target network environments.

Lack of standard security evaluation: A key problem in most of the existing security protocols is lack of standard evaluation criteria. Since several solutions are based on different evaluation criterion, it is not feasible to compare and analyze their security performance. Also, lack of standard platform for performance evaluation further detriments the study. Different simulators used with different simulation metrics do not provide accurate results.

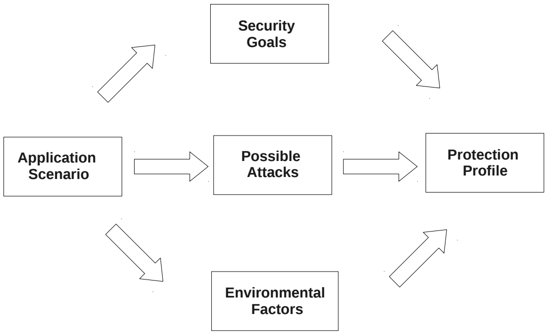

Fig. 1. Components comprising a protection profile. An application scenario embodies the security goals, possible attacks and environmental factors. These three compose the protection profile.

III. Protection Profile of Network Scenarios

Current secure routing protocols use a range of security mechanisms to address different security threats in ad hoc networks. However, as discussed in the previous section, existing key management and secure routing protocols do not provide solutions against all possible security threats. Existing methods are often unrealistic as they are independent of the network and environmental assumptions and hence lack the capability to act as stand-alone secure protocols in these networks. In order to ensure complete security solutions, it is necessary to design a framework that can clearly define a consistent set of policies and procedures needed to protect the network systems.

Common Criteria Model: The structural formation of our framework is inspired by the notions of the *Common Criteria* [6], the federal criteria for information technology security evaluation. The Common Criteria introduced the notions of protection profiles and security targets. According to the framework, a user would generate a protection profile to detail the protection needs, both functional and assurance, for a specific situation or a generic scenario. The protection profile would be abstract specification of the security aspects needed in an information technology product. The idea of defining ad hoc security scenarios based on a realistic security framework is similar to that of a protection profile. In response to a protection profile, the vendor would then map the requirements of the protection profile in the context of the specific product onto a statement called a security target. The security target then becomes the basis for the evaluation.

IV. Components of Protection Profiles

Our classification framework comprises the protection profile that specifies the security requirements and objectives for varying ad hoc network scenarios. The framework components are shown in Figure 1. For any given application scenario, one can determine the security goals, possible attacks and environmental characteristics of that particular ad hoc network. Based on these components, one can identify a well-balanced protection profile for the ad hoc network application scenario in consideration. Below, we describe each of the components in our classification framework.

A. Application scenario

Due to their minimal configuration and rapid deployment, ad hoc networks are suitable for use in various applications ranging from battlefield combat scenarios to sensors collecting patients data in a hospital. The prime component of our framework is application scenario as it forms the basis for developing a security solution. Security requirements, network characteristics and possible security threats vary depending on the intended use of ad hoc network applications. Hence, security solutions must be developed to adapt to the needs of different ad hoc network based applications.

B. Security Goals in Ad hoc Networks

As with traditional networks, to secure ad hoc networks, it is essential to consider the following attributes: confidentiality, integrity, authentication, availability and non-repudiation. These attributes define the security goals in a network.

Confidentiality (CONF): Confidentiality guarantees that the transmitted information is not disclosed to unauthorized entities. It ensures that the routing data from the source node must be accessible only to the intended destination. Leakage of sensitive information to adversaries may have disastrous consequences. Hence, care must be taken such that even if the information is tapped by an adversary, the information is not easily decipherable, thus assuring confidentiality. The most common security mechanism for achieving confidentiality is encryption. Encryption transforms a message into a ciphertext using an encryption key. Some of the most popular cryptographic encryption methods are Public Key Infrastructure (PKI) and symmetric key encryption. In wireless networks, nodes use cryptographic keys to encode and decode confidential messages.

Integrity (INTG): Information integrity ensures that the transmitted message is not altered or corrupted. When a message is transmitted in wireless medium, the data can be modified, tampered or deleted by malicious nodes in the network. The most significant security requirement for the routing mechanism concerns integrity. In case of military applications, routing information may be tactical information of primary importance. Thus, while considering security for routing control messages, we mostly consider how to generate and verify digests or digital signatures. The most popular techniques used to achieve integrity include Checksum, Cyclic Redundancy Check (CRC), Message Authentication Code (MAC) and Message Integrity Code (MIC). In wireless channels, MAC/MIC are more commonly used to verify data integrity.

Authentication (AUTH): Authentication provides the ability to identify a node and prevent node impersonation. Without authentication, a node in a wireless network can easily masquerade as another node gaining unauthorized access to the network resources. Common methods used for authentication are username-password, shared secret verification and biometrics.

Availability (AVAL): Availability ensures the survivability of the network under the presence of Denial-of-Service (DoS) attacks. It is important for a network to remain operational at all times to keep the network services and resources available to legitimate users. DoS and routing attacks targeting network availability can be mitigated by use of hash chains. For instance, hash chains can be used for numbering the packets. By limiting the number of packets by hash or cryptographic chains, DoS attacks such as flooding can be prevented. Intrusion detection mechanisms can also be used to detect attacks affecting availability. For example, the Watchdog mechanism can be used to promiscuously listen to the wireless medium and detect next hop node misbehavior. This method is used to detect packet drops in the network. Similarly, the Pathrater detection mechanism uses an average of the nodes' rating to evaluate the quality of the path to detect misbehavior. Path quality rating is compiled from link breaks, active nodes (where a packet was successfully sent in a previous time interval) and watchdog accusations. In general, it is possible to detect and isolate misbehaving and selfish nodes in an ad hoc network through intrusion detection techniques. Particular attacks that may be detected using these solutions are Black Hole [17], Wormhole [18] and Byzantine [19] attacks.

Non-repudiation (NREP): Non-repudiation guarantees that the sender of a message cannot later deny having sent the message. Digital signatures, a mechanism using PKI can be used as a process to provide NREP. However, the calculation overload should be taken in consideration when deployed in ad hoc networks.

C. Attacks on Ad hoc Networks

In this section, we present some of the attacks that target the above mentioned security goals in ad hoc networks.

Attacks targeting confidentiality (ACONF): In this attack, a malicious node can intercept and receive conversations of legitimate nodes. Since the wireless communication medium is broadcast in nature, transmitted messages can be easily overheard and fake messages injected into the network.

Authentication attacks (AAUTH): Impersonation or spoofing is a type of attack where the adversary assumes the identity of an authorized node. By impersonating another node, the adversary can receive data transmitted to the nodes and gain access to network resources that may not be available to them under normal circumstances.

DoS attacks (AAVAL): This type of attack is launched to deny network access to authorized entities. A simple DoS attack can be launched by flooding packets to targeted node(s) in the network. In wireless networks, DoS attacks can be launched at multiple protocol layers. In physical and MAC layers, an adversary could employ jamming signals to disrupt the on-going transmissions on the wireless channel. In the network layer, an adversary can exploit the routing protocol to disrupt the normal functioning of the network. In higher protocol layers, a malicious node could bring down critical services such as the key management service.

Environmental attacks (AENVR): In hostile environments, a malicious node can launch various routing attacks to disrupt routing operations or deny service to the network. Below, we list some of the routing attacks in ad hoc networks affecting network availability: (a) *Routing Table overflow*: In this attack targeted on table driven routing protocols, a malicious node advertises routes to non-existent nodes in the network thereby filling up routing tables and resources of legitimate nodes in the network. An adversary performs routing table poisoning by sending fictitious routing updates or modifying genuine route update packets sent to other uncompromised nodes. In packet replication, the malicious node replicates stale packets consuming additional bandwidth and battery power resources. (b) *Wormhole attack*: In this attack, a pair of colluding attackers receives and records packets at one location and replays them at another location in the network. Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. (c) *Black hole attack*: In this attack, an adversary falsely advertises shortest path or stable path to the destination node during the route discovery process. The intention of this attack is to disrupt the path-finding process or to intercept all data packets being sent to the destination node concerned. (d) *Byzantine attack*: A group of intermediate malicious nodes works in collusion and creates routing loops, routing packets to non-optimal paths, or dropping packets. This attack is difficult to detect as the network seems normally operational to the other nodes.

D. Environmental Factors

Different applications of ad hoc networks have varying network characteristics. For instance, nodes in these network may differ in terms of mobility, resource constraints and bandwidth requirements. Secure routing protocols used in such networks should take these fundamental differences into consideration. Hence, in our scenario centric framework, environmental assumptions acts as a critical component necessary for modeling and developing secure routing protocols according to the demands of the target network. The following environmental factors are considered:

- GPS Capability: Yes (GCAP), No (GDIS)
- Backbone Infrastructure: Yes (BBP), No (BBA)
- Node Capability: High (NCH), Low (NCL)
- Energy Constraints: High (ELH), Low (ELL)

Table I summarizes these environmental factors for different network scenarios.

TABLE I
ENVIRONMENTAL FACTORS FOR DIFFERENT SCENARIOS

Scenario	GPS Capability	Backbone Infrastructure	Node Capability	Energy Constraints
TANET	Yes	Yes	High	Low
VANET	Yes	Yes	High	Low
AANET	Yes	No	High	Low
WSANET	No	No	Low	High
UWANET	No	No	Low	High
CDNET	No	No	Low	High
BANET	No	No	Low	High
FRANET	Yes	Yes	Low	High

E. Protection Profile

A protection profile is used to define and specify security requirements for a given system to address the problems without dictating how these requirements will be implemented. It is often a combination of threats, security objectives, assumptions, security functional requirements, security assurance requirements and rationales. Since ad hoc networks are deployed in different applications and varying network scenarios, protection profiles can be used to define security requirements and protection needed to secure these networks. It is possible that a security breach in any layer can facilitate a potential attack on the entire wireless network. Secure routing protocols in ad hoc networks should be based on the protection profile to specify the type of protection suitable for the network in consideration. Specifically, the protection profile for secure routing in ad hoc networks comprises the following items:

- Assumptions about security aspects of the environment in which ad hoc network is deployed,
- Security threats to be addressed by the network,
- Security goals and objectives for the network, and
- Rationale demonstrating how the requirements meet the security goals, and how the security goals address the threats.

V. Protection Profile Examples

A protection profile comprises a range of security mechanisms that can used to meet the security objectives of different wireless ad hoc networks. Below, we describe some of these according to the scenario.

Tactical Ad hoc Network (TANET) is a network formed for communication among soldiers in a tactical operation. It is not feasible to set up a fixed or wired network for communication in a hostile environment such as the battlefield. TANET provides a required communication mechanism in this kind of environment. Due to the sensitive nature of communication involved in the tactical battlefield, these networks require the highest level of security and reliability. The TANET environment is comprised of heterogeneous nodes such as low-capability sensors, medium-capability nodes for data delivery, or high-performance nodes with directional antennas that relay network traffic via satellite links or airborne backbone network. Hence, in most cases, connection with a central server is possible for certification, authentication and security credential update. Also, since nodes in these networks are often equipped with GPS, it enables accurate localization and position estimation.

All five aspects of security goals are required for the nodes in TANET. Due to the nature of tactical operations, confidentiality of any message exchanged is of topmost priority. Only authenticated nodes should be able to communicate with each other and integrity of the message should also be ensured. Nodes should maintain their availability for communication and measures should be taken so that nodes cannot repudiate a transaction. Location privacy should also be maintained.

Vehicular Ad hoc Network (VANET) provides communication among vehicles to exchange information such as traffic, weather, road condition and accidents. VANET allows vehicles to avoid problems either by taking cautionary actions or alerting the driver.

Nodes in VANET are characterized by high mobility and driver behavior. These networks do not have a fixed infrastructure and hence rely on vehicles for network functionality. Vehicular nodes communicate with road side controllers which in turn exchange information with some central authority. Due to sufficient power supply from car batteries, energy efficiency is not an issue in VANETs.

The confidentiality requirement in VANET is flexible compared to TANET. However, only legitimate nodes should be allowed to communicate with each other and messages should be exchanged intact ensuring integrity.

Airborne Ad hoc Network (AANET). In this kind of network, network devices such as routers and transceivers are carried on high altitude aircrafts and uninhabited aerial vehicles (UAV). These networks sometimes act as the backbone for terrestrial ad hoc networks such as TANET.

Airborne network nodes are mobile with high velocity. They often use ground stations or satellite links for communication. GPS based localization and position estimation is available in this network as well. Nodes in this network maintain constant communication with a trusted central authority.

As this kind of network mostly works as a backbone for other ground ad hoc networks, availability is the topmost priority. Only authenticated nodes should be allowed to participate in the network. Integrity of the message should also be ensured.

Wireless Sensor Ad hoc Network (WSANET). Wireless sensor motes collecting data in different environments such as volcanic eruption and firefighting form this kind of ad hoc network. Data collected by the motes are sent to a central node for further processing.

Nodes in this network are inherently resource constrained with low processing speed, storage capacity and limited communication bandwidth. Once deployed, sensor nodes remain static in most cases.

The main task of nodes participating in this network is data aggregation. So, ensuring integrity of messages is of paramount importance. Also, non-repudiation mechanisms should be forced to find out if any node is sending bogus values.

Underwater Ad hoc Network (UWANET) networks are formed for localized monitoring and coordinated networking amongst a large amount of underwater nodes. Currently, UWANET is widely used for uninhabited ocean monitoring.

Underwater networks differ from generic ad hoc and sensor networks in terms of huge propagation delay, low bandwidth and use of acoustic signals for communication. Sometimes, they also use autonomous underwater vehicles for better communication. Nodes in these networks often have low or medium mobility due to environmental water current. Nodes in this network can depend on surface stations for security operations. However, due to resource constraints, node level processing of cryptographic operations may not be feasible.

Nodes in this network are also data collecting sensors. Maintaining integrity is very important in this network as well. Only authenticated nodes should participate in the network.

Collaborative and Distributed Ad hoc Network (CDANET) fulfills the requirement of applications that need temporary communication with minimal configuration among a group of people in a class or conference. For example, researchers in a conference can use this network to exchange presentations. An instructor in a classroom can use CDANET for distributing lecture materials.

Nodes in this network are often laptops and personal hand held devices. However, due to the sporadic nature of this network formation, assuming the presence of any central authority might not be a feasible option.

As this network is formed to share data among nodes of a certain group, there should be mechanisms in place to block outsider nodes from participating in network activities. Integrity of the exchanged data should also be ensured.

Body Area Ad hoc Network (BANET) consists of mobile sensors implanted on the body that communicate with each other to monitor vital body parameters. BANET is mostly used at hospitals to monitor critical patients.

Small medical sensors are often used in this kind of ad hoc network. These nodes can possess shared secrets before deployment, but due to resource constrained sensor devices, we cannot perform expensive cryptographic computation on these nodes.

In most cases, data in this network is very sensitive and highly private medical information. So, mechanisms ensuring both confidentiality and integrity should be in place. Also, authentication should be done before any network operation is executed.

First Responder Ad hoc Network (FRANET). During disaster or accidental emergency scenario, this kind of network helps first responders to communicate with each other and exchange information. Other emergency scenarios include search and rescue, crowd-control and fire-fighting.

Nodes in this network are heterogeneous. Some of these are hand held devices used by the first responders. These hand held devices communicate with the sensors measuring the condition of the injured. Devices held by the responders can communicate with a central authority, but sensors do not have that capability.

The emergent characteristic of this network requires solid mechanisms to ensure availability. Also, confidentiality should be maintained as the data is the vital information of injured persons in most cases.

VI. Protection Profile based taxonomy of Secure Routing Protocols

In this section, we classify the secure routing protocols according to the protection profiles of different scenarios. According to our investigation, most of the protocols are not a perfect fit for the protection profile of a given scenario. However, we have found that the combination or slight modification of existing protocols makes them a close fit for the scenarios.

Tactical Ad hoc Network (TANET): The SPAAR protocol provides confidentiality, integrity, authentication and non-repudiation. The environmental assumption of this scenario such as the presence of GPS is also suitable for the operation of this protocol. However, to address routing misbehavior, either CONFIDANT or Watchdog-Pathrater should be used. Packet leashes should be used to address wormhole attacks.

Vehicular Ad hoc Network (VANET): The environmental assumption and protection profile of VANET makes ARAN and SAODV suitable for the dynamically changing nature of the network. Both of them are on-demand routing protocols. However, availability related attacks are not addressed in these routing protocols. On the other hand, the SPAAR protocol can also be used in this network if the vehicle is GPS enabled.

Airborne Ad hoc Network (AANET): A SLSP routing protocol providing authentication, integrity and non-repudiation is suitable for this scenario. As this network works mostly as a backbone network, the network topology does not change frequently. So, a link state routing protocol meeting the requirements of the protection profile is a good fit for AANET. SLSP also provides protection from availability related attacks such as DoS attack, which is critical for a backbone network.

Wireless Sensor Ad hoc Network (WSANET): Although multiple secure routing protocols meet the security goals of WSANET protection profile, environmental characteristics of this network makes them an infeasible choice for it. However, by using a lightweight shared secret pre-deployed among participating nodes, SEAD- and ARIADNE-like protocols might be a close fit for this scenario. However, protocols such as ARAN and SLSP that need access to a central authority for their function are not suitable for this scenario.

Underwater Ad hoc Network (UWANET): Similar to WSANET, with the existence of a pre-deployed shared secret, SEAD- and ARIADNE-like protocols might be used in this type of network as well. When autonomous underwater vehicles are present, central authority based protocols might be used.

Collaborative and Distributed Ad hoc Network (CDANET): SAODV closely fits the protection profile of the scenario. In addition, a simple routing protocol using MAC or MIC along with a shared secret works for the CDANET protection profile.

Body Area Ad hoc Network (BANET): Although, SPAAR meets the security goals of BANET's protection profile, the environmental assumption of this network makes SPPAR an infeasible solution for this network. Shared secret based lightweight symmetric encryption in conjunction with MAC/MIC can be used in a routing protocol to fit the protection profile of this network.

First Responder Ad hoc Network (FRANET): The Protection profile of this network makes SPAAR a good choice for this scenario if the hand held devices of first responders are GPS enabled. In absence of GPS, shared secret based integrity and confidentiality measures should be taken.

VII. Comparison with Existing Classification Methods

In [4], Deng, Li, and Agrawal have discussed the existing secure routing protocols based on attacks those protocols address. For example, SEAD provides robust security against routing attacks targeting the sequence number and routing metrics. Ariadne can defend against routing and wormhole attacks. The ARAN protocol can defend against authentication and repudiation attacks. However, we remark that this kind of

TABLE II
SUMMARY OF SCENARIO CENTRIC PROTECTION PROFILE. CWP REFERS TO THE COMBINATION OF CONFIDANT, WATCHDOG AND PATHRATER.

Scenario	Security Goals	Attacks	Environmental Factors	Protocol
TANET	CONF, AUTH, INTG, AVAL	ACON, AAUTH, AINTG, AAVAL, AENVR	GCAP, BBP, NCH, ELL	SPAAR+CWP
VANET	AUTH, INTG, AVAL	AAUTH, AINTG, AAVAL, AENVR	GCAP, BBA, NCH, ELL	SPAAR, ARAN, SAODV+CWP
AANET	AUTH, INTG, AVAL	AAUTH, AINTG, AAVAL, AENVR	GCAP, BBA, NCH, ELL	SLSP
WSANET	AUTH, INTG, AVAL	AAUTH, AINTG, AAVAL, AENVR	GDIS, BBA, NCL, ELH	N/A
UWANET	AUTH, INTG, AVAL	AAUTH, AINTG, AAVAL, AENVR	GDIS, BBA, NCL, ELH	N/A
CDNET	INTG, AVAL	AINTG, AAVAL, AENVR	GDIS, BBA, NCL, ELH	SAODV
BANET	CONF, AUTH, INTG, AVAL	ACON, AAUTH, AINTG, AAVAL, AENVR	GDIS, BBA, NCL, ELH	N/A
FRANET	CONF, AVAL	ACON, AAVAL, AENVR	GCAP, BBA, NCL, ELH	N/A

approach does not give an overall view of the domain and might not be complete as a classification approach.

In [3], Yih-Chun and Perrig have classified the existing secure routing protocols based on the base routing protocol those protocols follow such as DSR [11], AODV [14] and DSDV [9]. For example: SEAD is based on DSDV. SAODV and ARAN are security extensions to AODV. Protocols like Ariadne and CONFIDANT are based on DSR. This classification approach also lacks in completeness and extendibility.

Fonseca and Festag [20] have classified current secure routing protocols based on security mechanisms used by the protocols such as:

- Asymmetric cryptography: ARAN, SPAAR and SLSP.
- Symmetric cryptography: SEAD and ARIADNE.
- Hybrid approach: SAODV.
- Reputation mechanisms: CONFIDANT and Watchdog-Pathrater.

Now, we compare these classification approaches to our approach in terms of the following metrics:

Completeness: This metric measures to what extent the taxonomy provides a complete overview of secure routing protocols in the ad hoc networks domain. As we have discussed earlier, the existing classification or taxonomic criteria fail to capture the fact that an ad hoc network can manifest itself in different forms. On the contrary, our approach is based on the scenario-centric protection profile, thus covering most of the application scenarios in existing literature.

Usability: This metric is used to measure how simple it is to choose a protocol for an application scenario. Classification mechanisms discussed earlier in this section clearly show that it is very difficult to choose a protocol based on such classification. Although, given an application, an expert might decide whether to use an asymmetric or symmetric approach; absence of environmental factors in the classification criteria hinders the usability of these classification mechanisms. On the other hand, our approach is based on a protection profile where the application scenario is the first consideration making it more usable than the existing ones.

Extendibility: By this metric, we wanted to measure whether this taxonomy could be extended to help the design of new secure routing protocols for ad hoc networks. The protection profile of different scenarios clearly defines the security needs of a specific scenario. By adhering to the protection profile, new secure routing protocols can be designed efficiently. This feature is almost completely absent in the existing classification approaches.

VIII. CONCLUSION

In this paper, we presented an efficient taxonomy of existing secure routing protocols in different ad hoc network scenarios. We also discussed the suitability of several secure routing protocols for those scenarios. From the taxonomy, it is clear that quick responses are necessary in domains such as body sensor, first responder and underwater ad hoc networks. To facilitate the design of new secure routing protocols, the protection profile of different application scenarios proposed in this work can be a good starting point for researchers.

REFERENCES

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Mobile Computing and Networking*, 2000, pp. 255–265.

[2] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *SIGMOBILE Mob. Computer Communication Review*, vol. 6, no. 3, pp. 106–107, 2002.

[3] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," *Security & Privacy, IEEE*, vol. 2, no. 3, pp. 28–39, May-June 2004.

[4] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 70–75, Oct 2002.

[5] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002, pp. 226–236.

[6] "Common criteria: The common criteria portal," 2011. [Online]. Available: http://www.commoncriteriaportal.org/

[7] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *ICNP '02: Proceedings of the 10th IEEE International Conference on Network Protocols*, Washington, DC, USA, 2002, pp. 78–89.

[8] Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY*, June 2002, pp. 3–13.

[9] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21–38, 2005.

[11] D. Johnson, "Routing in ad hoc networks of mobile hosts," in *Proceedings of the Workshop on Mobile Computing Systems and Applications*, Dec 1994, pp. 158 –163.

[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, 2002.

[13] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *SAINT-W '03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, 2003, p. 379.

[14] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," RFC Editor, United States, 2003.

[15] S. Carter and A. Yasinsac., “Secure position aided ad hoc routing protocol,” in *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, Cambridge, MA, USA, November 2002, pp. 329–334.

[16] Y.-C. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 3, pp. 1976–1986, 2003.

[17] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black hole attack in mobile ad hoc networks,” in *Proceedings of the 42nd annual Southeast regional conference*, ser. ACM-SE 42. New York, NY, USA: ACM, 2004, pp. 96–97.

[18] M. Khabbazian, H. Mercier, and V. K. Bhargava, “Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks,” *Trans. Wireless. Comm.*, vol. 8, pp. 736–745, February 2009.

[19] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Trans. Program. Lang. Syst.*, vol. 4, pp. 382–401, July 1982.

[20] E. Fonseca and A. Festag, “A survey of existing approaches for secure ad hoc routing and their applicability to vanets,” NEC Network Laboratories, Heidelberg, Germany, Tech. Rep., March 2006. [Online]. Available: http://www.network-on-wheels.de/downloads/survey_sec_routing_v1-1_cite.pdf