Zusammenfassung der Dissertation:
Effiziente kryptographische Protokolle für kabellose Maschennetzwerke

Diese Dissertation beschäftigt sich mit der Entwicklung eines vollständigen und effizienten Sicherheitskonzeptes für Wireless Mesh Netzwerke (WMN). In einem Schritt für Schritt Ansatz beginnen wir zunächst mit der Analyse der speziellen Netzwerkcharakteristik von WMN, welches uns eine Auswertung, Verbesserung und das Erstellen von kryptographischen Lösungen erlaubt, die gezielt auf Wireless Mesh Netzwerke abgestimmt sind.

Es hat sich herausgestellt, dass Gruppenschlüsselaustauschprotokolle (GKA) effizienter für Wireless Mesh Netzwerke sind, als paarweise Schlüsselsysteme (vorgeschlagen durch den IEEE 802.11s Standard). Daher konzentriert sich diese Arbeit auf den Einsatz von GKA Protokollen, um ein effizientes Sicherheitskonzept zu realisieren. Weiterhin führen wir zwei verschiedene Modelle für die Performanzmessung in WMN ein. Beide Modelle werden verwendet, um die Perfomanz von drei repräsentativen GKA Protokollen zu untersuchen. Die Messungen zeigen, dass das Tree Based Key Agreement (TBKA) Protokoll die beste Performanz in WMN bietet.

Mit dem Wissen über die spezielle Netzwerkcharakteristik von WMN waren wir darüberhinaus in der Lage, eine verbesserte Version von Burmester-Desmedt II (BD2) zu entwickeln, das durch seine gezielte Anpassung bessere Ergebnisse als das TBKA Protokoll liefert. Praktische Messungen der getesteten Protokolle bestätigen die Ergebnisse und zeigen die Praktikabilität der beiden Performanzmessmodelle.

Eine zusätzliche Erweiterung der GKA Protokolle erlaubt einen Einsatz unter realen Bedingungen. Das bedeutet, dass die erweiterten Varianten in WMN arbeiten, bei denen die Topologie nicht a priori bekannt ist. Als nächster Schritt wird dem effizientesten praktischen GKA Protokoll eine Authentifizierungserweiterung hinzugefügt. Durch das Hinzufügen der Authentifizierung entsteht ein Authenticated Group Key Agreement (AGKA) Protokoll, welches zusätzlich über einen sicheren Routingalgorithmus verfügt.

Mit dem entstandenen AGKA Protokoll und einigen zusätzlichen Protokollnachrichten für die Robustheit des Systems kann schließlich ein vollständiges Sicherheitskonzept für Wireless Mesh Netzwerke realisiert werden. Das vollständige Sicherheitskonzept wurde in einem realen Testbett implementiert, um die praktische Nutzbarkeit des Konzeptes zu zeigen.

Andreas Noack, M.Sc.